The airline Passenger data disclosure case and the EU-US debate

Pérez Asinari, María Veroníca; Poullet, Yves

Published in:
Computer Law and Security Report

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

The Airline Passenger Data Disclosure Case and the EU-US Debate

María Verónica Pérez Asinari* and Yves Poullet**
Centre de Recherches Informatique et Droit (CRID)
University of Namur
Belgium
http://www.crid.be
September 2003

Introduction

In the aftermath of the events of 11th September 2001, decisions have been taken unilaterally by US authorities requiring air line companies to provide direct access or transfer of data concerning passengers and cabin crews flying to, from or within the US to certain US administrations. These decisions have been challenged by EU authorities insofar they constitute a violation of EU privacy and personal data protection law which is considered to be of public order. The debate is still pending.

The present paper will comment on this complex and multi-featured discussion opposing two fundamental societal values: on the one hand, the right of the citizens to be protected from terrorism and the obligation of a sovereign State to fight against it and safeguard public security[1], and on the other hand, the individuals' right to personal data protection and privacy and the obligation of the EU, in the light of international and supranational commitments, to protect them in this arena. After a short presentation of

*Researcher
**Dean of the Faculty of Law, Director of the CRID.

This article expresses the own views of the authors. In no way might it be interpreted as the opinion of the organisations to which they belong.

We would like to thank Jean-Marc DINANT, researcher at the CRID, for his clarifying comments.

[1] In the EU, the fight against terrorism is one of the specific objectives mentioned in Article 29 TEU. The Framework Decision of 13 June 2002 on combating terrorism, OJCE L 164, 22.6.2002, has declared: "Whereas: (1) The European Union is founded on the universal values of human dignity, liberty, equality and solidarity, respect for human rights and fundamental freedoms. It is based on the principle of democracy and the principle of the rule of law, principles which are common to the Member States. (2) Terrorism constitutes one of the most serious violations of those principles. The La Gomera Declaration adopted at the informal Council meeting on 14 October 1995 affirmed that terrorism constitutes a threat to democracy, to the free exercise of human rights and to economic and social development. (…)".

the US decisions and their context (Point I), the authors will analyse the EU position, its claim for an adequate personal data protection to be ensured by the US authorities and the legal grounds for this position (Point II). Finally, a synthetic approach to the adequacy of the US decisions *vis-à-vis* the EU legal provisions will be proposed (Point III).

I. The US legal framework

I.1. The legislative context

Directly after the tragedy of 11th of September 2001, the US Government took a great amount of initiatives to fight against terrorism. The Patriot Act[2], which is commonly known, is one example. However, more specific legislation has been enacted as well, in order to tackle the risks created by the terrorist threat.

In the immigration and admission of aliens sphere, the Enhanced Border Security and Visa Entry Reform Act[3] was enacted on 14th May 2002. As regards air transportation, the US adopted the Aviation and Transportation Security Act (ATSA)[4] on 19th November 2001. This Act has been followed by secondary regulations, notably the document "Passenger and Crew Manifests Required for Passengers Flights in Foreign Air Transportation to the United States", published in the Federal Register on 31st December 2001[5], and the document "Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States", published in the Federal Register on 25th June 2002[6].

---

[2] 107th Congress, 24th October 2001. The PATRIOT Act has been extensively analysed. Whereas certain sectors consider that it "eliminated the checks and balances that previously gave courts he opportunity to ensure that these powers were not abused" (Electronic Frontier Foundation "EFF Analysis of the Provisions of the USA PATRIOT Act", 31st October 2001, available at: http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.php , last visited 08/03/02), others argue that "the common wisdom on the USA Patriot Ac is incorrect. The Patriot Act did not expand law enforcement powers dramatically, as its critics have alleged. In fact, the Patriot Act made mostly minor amendments to the electronic surveillance laws" (O. KERR "Internet Surveillance Law After the USA PATRIOT Act: the Big Brother that isn't", The George Washington University Law School, Public Law and Legal Theory Working Paper No. 043, available at: http://ssrn.com/abstract=317501).

[3] Public Law 107-173, 107th Congress.

[4] Public Law 107-71, 107th Congress.

[5] Department of Treasury, Customs Service, (66 FR 67482) T.D. 02-01.

[6] Department of Treasury, Customs Service, (67 FR 42710) T.D. 02-33.

The main purpose of all this legislation is to enhance security for the fight against terrorism and create what the US authorities have called a "21st Century Smart Border"[7]. In order to achieve this goal, the Government and Parliament have given a very large mandate to a new public body: the Transportation Security Agency (TSA), which is part of the Department of Homeland Security[8], to take appropriate measures in order to improve aviation security.

One of the most important decisions taken in this context was to use information technology, particularly risk analysis tools, for detecting terrorists. All the data transmitted by the air transportation companies will be centralized in a large database, operated both by US Customs and Immigration and Naturalization Services. Furthermore, a Computer Assisted Passenger Pre-screening Program (CAPPS II) is cretaed to evaluate all passengers before they board an aircraft. We will comment more extensively on these initiatives in what follows.

I.2. The measures

The above referred regulations have created different obligations for air carriers, which derive also in different information management systems, either centralized or not.

The Advanced Passenger Information System (APIS) deals with all the data requested from and transmitted by all air transportation companies. The ATSA stipulates the following:

> *"(1) IN GENERAL.- Not later than 60 days after the date of enactment of the Aviation and Transportation Act, each air carrier and foreign air carrier operating a passenger flight in foreign ain transportation to the United States shall privide to the Commissioner of Customs by electronic transmission a passenger and crew manifest containing the information specified in paragraph (2). Carriers may use the advanced passeger information system established under section 431 of the tariff Act of 1930 (19 U.S.C. 1431) to provide the information required by the preceding sentence.*

[7] See on that concept the declaration made by A. Hutchinson, under-secretary of Border and Transportation Security at the US Department of Homeland Security, while referring to the US VISIT system as part of the comprehensive information system that will provide the United States with a "smart border" that "expedites legitimate trade and travel, but stops terrorists in their tracks". This system "will be based on visas that include biometric features such as fingerprints and photographs to permit identification of foreign visitors when they arrive. (…) Through this 'virtual border' we will know who violates our entry requirements, who overstays or violates the terms of their stay, and who should be welcome again". She further expressed that these initiatives must not be considered as a way to exclude any immigrants, "[i]mmigrants still search for the American Dream. And when they find it, all American benefit", reported in "Hutchinson says new system provides America with 'smart border'", web site of the US Mission to the E.U, 19th May 2003, available at : http://www.useu.be/Terrorism/USResponse/May1903USVISITSystem.html , last visited 08/08/03.

[8] The TSA has been created under the ATSA.

(2) INFORMATION.- A passenger and crew manifest for a flight required under paragraph (1) shall contain the following information:

(A) The full name of each passenger and crew member.

(B) The date of birth and citizenship of each passenger and crew member.

(C) The sex of each passenger and crew member.

(D) The passport number and country of issuance of each passenger and crew member if required for travel.

(E) The United States visa number or resident alien card number of each passenger and crew member, as applicable.

(F) Such other information as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety"[9].

Paragraph (4) establishes that the passenger and crew manifest shall be transmitted to the Customs Service in advance of the aircraft landing in the US[10]. Furthermore, the following paragraph regulates on PNR:

"(3) PASSENGER NAME RECORDS.- The carriers shall make passenger name record information available to Customs Service upon request"[11].

As we have already seen, certain documents have been published in the Federal Register specifying these regulations. The Interim rule of 31st December 2001 has extended the required data elements for the manifests, for instance, by adding the obligation to transmit electronically to Customs *"(3) [t]he foreign airport where each passenger began his air transportation to the United States; for each passenger and crew member destined to the United States, the airport in the United States where the passenger and crew member will process through Customs and Immigration formalities; and for each passenger and crew member transiting through the United States and not clearing through Customs and Immigration formalities, the foreign airport of final destination for the passenger and crew member"*[12].

In what concerns PNR, the Interim rule of 25th June 2002 states, among other issues, that *"[i]n order to readily provide Customs with such access to requested PNR data, each air carrier must ensure that its electronic reservation/departure control systems correctly interface with the US Customs data Center, Customs Headquarters"*[13]. It is clear then, that these data will not be "transferred" (as a first step, see *infra*) but directly "accessed" on-line.

---

[9] Sec. 115. Passenger Manifest, paragraph (c). Amendment to 49 USC 44909.

[10] The Interim rule of 31st December 2001 states that this transfer should be made "not later than 15 minutes after the departure of the aircraft from the last foreign port or place", p. 67483.

[11] Sec. 115. Passenger Manifest, paragraph (c). Amendment to 49 USC 44909.

[12] See p. 67483.

[13] See p. 42710.

The Interim rule we are commenting further mentions, "merely to be illustrative", certain data elements to which Customs may request access in relation to a passenger[14]:

> (1) Last name; first name; date of birth; address(es); and phone number(s);
> (2) Passenger name record locator (reservation) number;
> (3) Reservation date (or dates, if multiple reservations made), or if no advance reservation made ("go show");
> (4) Travel agency/agent, if applicable;
> (5) Ticket information;
> (6) Form of payment for ticket;
> (7) Itinerary information;
> (8) Carrier information for the flight, including but not limited to: carrier information for each segment of the flight if not continuous; the flight number(s); and date(s) of intended travel;
> (9) Seating; and
> (10) PNR history[15].

Indeed, PNR data contains other information, some of them of sensitive nature. PNR, for instance, stores the requested kind of food for the flight (this food can have health, philosophical or religious connotations), whether any facilities for disable are needed[16], etc. It also stores who will pay for the bill (company, association, university, public body, party, etc.) and even in relation to which internal account (what is normally connected to a specific client, project, etc.). The itinerary field includes all air space and related non-airline, auxiliary services the passenger requested.[17]

---

[14] See p. 42711.

[15] The history of PNR contains changes and deletions to a PNR from the date it was created (footnote added by the authors).

[16] Under the PNR system, those fields are called SSR (Special Service Request).

[17] For a practical description of PNR see: "Lesson: Passenger Name Record", Advanced Worldspan, available at: http://globallearningcenter.wspan.com/emealearningcenter/PDFs/Student%20Workbooks/210/1101%20PNR%20Lesson.pdf , last visited 02/09/03. See also: E. HASBROUCK "Total Travel Information Awareness", available at: http://hasbrouck.org/articles/travelprivacy.html , last visited 18/08/03. In this article we read: "Passenger Name Records (PNR's) maintained by airlines, computerized reservations systems or "global distribution systems" (CRS's/GDS's), and travel agencies don't just contain flight reservations and ticket records. They include car, hotel, cruise, tour, sightseeing, and theater ticket bookings, among other types of entries. PNR's show where you went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a particular other person, they show whether you asked for one bed or two. Through departmental and project billing codes, business travel PNR's reveal confidential internal corporate and other organizational structures and lines of authority and show which people were involved in work together, even if they travelled separately. Particularly in the aggregate, they reveal trade secrets, insider financial information, and information protected by attorney-client, journalistic, and other privileges. Through meeting codes used for convention and other discounts, PNR's reveal affiliations -- even with organizations whose membership lists are closely-held secrets not required to be divulged to the government. (…)". More specifically on PNR, by the same author, see: "What's in a Passenger Name Record (PNR)?", available at: http://hasbrouck.org/articles/PNR.html , last visited 18/08/03.

Another system to be implemented is the US VISIT[18], which consists in a systematic scanning of the travel documents of each US visitor. Photo and fingerprints will be taken and the data so obtained will be checked against lists of those who should be denied the entry within the US territory for different reasons (terrorism, criminal violations, illegal entry, visa violations)[19]. This system will permit to centrally process personal data including certain data based on biometric features[20] (today digital photo and fingerprints tomorrow facial recognition and iris scans)[21] . In order to facilitate this work, visa waiver countries are required to use tamper-proof passports that include biometric identifiers from August 2004. This data will not be requested to airline companies, so, we will not develop this aspect in the present paper. However, we are of the opinion that its existence had to be mentioned here insofar US regulations would permit interconnections between the PNR data and the data generated in the context of the US VISIT program.

The TSA is authorized, apart from to use the data collected through these two sources, to establish a "watch-list" of individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety"[22]. Furthermore, the different airline companies are operating the Computer Assisted Pre-screening Program (CAPPS), a passenger–screening tool, in order to identify passengers for enhanced screening before their boarding.

An updated version of CAPPS[23], CAPPS II, is presently being developed for providing a more efficient identification of terrorist risks. "Essentially, CAPPS II process will be a passive system that produces a general indication of the level of terrorist risk each airline passenger might pose to civil aviation security. It will be activated by a traveller's airline reservation request. Airlines will ask passengers for specific reservation information that will include passenger's full name, plus other identifiers including date of birth, home address and home phone number. Passengers will not be asked to provide social security numbers, and TSA will not look at credit worthiness. The CAPPS II process will then authenticate each passenger's identity through publicly and commercially available databases. Once a passenger's identity is authenticated and the passenger's information is run against terrorist or appropriate Federal Government

[18] Planned to be implemented from January 2004.

[19] $400 million have been foreseen by the Congress to set up the system.

[20] For a European view regarding biometrics see: Article 29 Data Protection Working Party, Working Document on biometrics, 1st August 2003, WP 80, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf

[21] On all that see "Hutchinson says…", *op.cit.*

[22] In fact, documents obtained by EPIC demonstrate the existence of two lists: the "No-Fly" watchlist and the "selectee" list regarding persons submitted to additional security measures. The criteria for putting a name into the list remain secret. See: EPIC "Documents show errors in TSA's 'No-Fly' watchlist", April 2003, available at: http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html , last visited 08/08/03.

[23] The first CAPPS has been created after the Lockerbie bombing of a PanAM jet.

systems, an aggregate numerical threat score will be generated that TSA will use to determine which passengers should proceed through the ordinary screening process and which passengers should be asked to a somewhat more thorough screening. In extremely rare cases, the system may identify an individual who is a known foreign terrorist or the associate of a known foreign terrorist. In such a case, law enforcement authorities would be notified and given the opportunity to take appropriate action".[24]

All these systems will be operated under the control of the TSA. Privacy issues are not absent of the implementation of all these systems. The administrator of the TSA, James M. Loy, said that the TSA is taking privacy issues into account as it develops CAPPS II: "CAPPS II will operate under a stringent privacy protection protocol being developed through discussions with privacy groups (…). Strict firewalls and access rules will protect a traveller's information from inappropriate use, sharing, or disclosure"[25].

According to the ATSA requirement, a Privacy Officer has been nominated in the US Department of Homeland Security[26] to implement privacy requirements and to control their respect. This Privacy Officer is member of the Department of Homeland Security.

It is quite obvious that all the measures described affect significantly data controllers[27] which are operating from foreign countries and create new risks for the protection of personal data with European origin. The data relates to travellers (more or less 12 millions of passengers) flying to US and the requirements of US government interfere with the national legislation applicable to airline companies' data processing activities in the foreign countries where the passengers make the reservation, buy the ticket, take the plane, etc., and put into question their sovereignty by operating far beyond the US borders. To justify this extraterritorial approach, US authorities have developed a new conception of their own sovereignty not limited to the physical borders: "[b]ut in the

[24] Statement of Admiral James M. Loy, Administrator of the Department of Homeland Security's Transportation Security Administration, before the House of Representatives Subcommittee on Technology and Information Policy, 6th May 2003, available at : http://www.useu.be/Terrorism/USResponse/May0603LoyITTransportSecurity.html , last visited 08/08/03.

[25] Statement of Admiral James M. Loy, Administrator of the Department of Homeland Security's Transportation Security Administration, before the House of Representatives Subcommittee on Technology and Information Policy, 6th May 2003, available at : http://www.useu.be/Terrorism/USResponse/May0603LoyITTransportSecurity.html , last visited 08/08/03. It has to be noted that from a European perspective, as we will see later on, the implementation of security measures is one of the obligations of data controllers, but certainly not the only one.

[26] This person is N.O'Connor Kelly, who was present at the Hearing organized by the European Parliament. She insisted on the fact that the creation of this position was a "historic development in privacy and data protection in US" insofar it marks the "first statutorily mandated, Congressionally created privacy officer for the Department of Homeland Security (…)", see the report at the United States Mission to the European Union website "US Officials Discuss Homeland Security, passenger name Record with EU", available at: http://www.useu.be/Terrorism/USResponse/May0603BrowingPNREP.html , last visited 08/08/03.

[27] The airline companies are subject to penalties in case they do not comply with the different US provisions.

21st Century, border security can no longer be just a coastline, or a line on the ground between two nations. It's also a line of information in a computer, telling us who is in the country, for how long, and for what reason… In the 21th Century it is not enough to place inspectors at our ports of entry to monitor the flow of goods and people. We must also have a 'virtual border' that operates far beyond the land border of the United States"[28]. This reasoning has been also held in the context of the ECHELON case[29], which is a UK-US system of electronic surveillance of the messages exchanged through satellites. The ECHELON system was, indeed, criticized by the European Parliament as violating the European fundamental right to privacy[30].

Notwithstanding, the TSA issued a notice narrowing the scope of the CAPPS II, published on the Federal Register on 1st August 2003[31]. This notice describes how the TSA will use CAPPS II and which changes have been made from the notice published at the Federal Register on 15th January 2003. Indeed, many comments and negative reactions were received in response to the prior Privacy Act notice. That has generated an obvious need to make some reforms in the proposal to make it data privacy compliance. For instance, whereas the original document on CAPPS II stated that information about individuals would be maintained for up to 50 years, the new notice expressed that for almost all passengers, that information will be deleted soon after the trip is safely completed, and for a "few risk" persons, the length of time the information will be kept is still under consideration.

I.3. Reactions in the US

"Jan Adams and Rebecca Gordon of California, for example, were detained at San Francisco International Airport, and told that their names appeared on the secret 'no-fly' list. The two women – peace activists who publish a newspaper called *War Times* – were told nothing about why they were on such a list, or how they could get off. The ACLU has filed suit against the Federal Government on their behalf to find out how the

---

[28] See the report "Hutchinson says new system provides America with 'smart border'", *op. cit.* As regards the modern notion of "sovereignty", see the developments and quotations, in Y. POULLET, "Pour une justification des articles 25 et 26 en matière de flux transfrontières", in *Liber amicorum B. De Schutter*, VUB Press, 2003, p. 280 and ss.

[29] About ECHELON see the Federation of American Scientists' website: http://www.fas.org/irp/program/process/echelon.htm. And the report Y. POULLET and J.M. DINANT, "Le réseau Echelon existe t'il ? Que peut-il faire ? Peut-on et doit-on s'en protéger ?" Report published by the Belgian Committee of Surveillance, 1999, p. 13 and ss., available at: http://www.droit.fundp.ac.be/textes/echelonfr.pdf

[30] See the European Parliament Resolution , 5th September 2001 and the Working Paper of the European Parliament temporary Committee on the Echelon Interception System (Schmidt Report), available at: http://fas.org/irp/program/process/europarl.draft.pdf.

[31] Department of Homeland Security, Transportation Security Administration, Docket No.DHS/TSA-2003-1, Privacy Act of 1974: Notice of Status of System of Records; Interim Final Notice; Request for Further Comments, (68 FR 45265).

'no fly' lists were created, how they are being maintained or corrected and, most importantly, how people who are mistakenly included on the list can have their names taken off. One question we believe needs answering is whether our clients are on the 'no fly' list because of their First Amendment protected political views".[32]

This is just an example of the role that civil liberties advocates are playing in the discussion on the implementation of the new measures. The Electronic Privacy Information Center (EPIC) had posted on its website several pages[33] with news about the debate on passenger data and the campaigns against the US policy. Moreover, they have submitted an action against the Department of Homeland Security, the Transportation Security Administration and the Department of Defense, under the Freedom of Information Act (FOIA), seeking the release of agency records concerning airline passenger screening procedures requested by EPIC from defendants.[34]

Indeed, EPIC sent a letter to the TSA on 10th March 2003 requesting records related to CAPPS II project addressing the following subjects: "(a) any existing legal, statutory and/or regulatory frameworks concerning governmental access to and use of transactional and other records about individuals. This request includes, but is not limited to, any assessments of the legal authority (or lack thereof) for information collection activities planned or proposed for the CAPPS II project; and (b) potential privacy and/or civil liberties implications of the activities planned or proposed for the CAPPS II project". The answer was delivered late and incomplete.

Apart from that, John Gilmore, a US citizen, filed a lawsuit against John Ashcroft (in his official capacity as Attorney General of the US) and other civil servants (with responsibilities in connected areas). Giving a frame to his action he said that he was "concerned that the climate of fear that currently pervades American society [is] eroding long-standing constitutional rights".[35] Basically, he challenged the "secret" character of a regulation limiting people right to travel anonymously and the use of "no-fly lists" that are created and maintained without transparency and control. In his complaint it is expressed: "[p]laintiff objects to the unregulated use of such lists because he believes history teaches that granting the government unlimited control over 'enemies list' will inevitably result in abuse". It is interesting to see the myriad of constitutional causes of action raised by the plaintiff.[36]

---

[32] Testimony of Barry Steinhardt, Director of the ACLU Technology and Liberty Program on Government Data Mining Before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, available at: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12669&c=206 , last visited 04/09/03.

[33] See the EPIC's website : http://www.epic.org/privacy/intl/passenger_data.html , last visit 22/08/03.

[34] EPIC v. DHS, TSA and DoD; United States District Court for the District of Columbia, available at: http://www.epic.org/privacy/airtravel/capps2-suit.pdf , last visited 02/09/03.

[35] John Gilmore v. John Ashcroft *et alii*, United States District Court Northern District of California, available at: http://cryptome.org/gilmore-v-usa-cid.htm , last visited 18/08/03.

[36] (1) Vagueness in Violation of the Due Process Clause of the Fifth Amendment of the United States; (2) Violation of the Right to be Free from Unreasonable Searches and Seizures in Violation of the Fourth Amendment of the United States Constitution; (3) Violation of the Right to Travel in Violation of the Due

Particularly in what concerns the First Amendment, it has been pointed out that "[f]ew activities implicate the assembly clause of the First Amendment as directly as travel. When people travel to assemble, as they do when they travel for business or organization meetings or conventions, or to meet friends and relatives, their travel is an act of assembly. Travel is not just an activity often engaged in for purposes protected under other clauses of the First Amendment (such as travel to petition the government for a redress of grievances, or travel for purposes protected as freedom of speech or of the press), but travel is, in and of itself, an activity directly protected under the assembly clause of the First Amendment".[37]

Even if the final decisions of the cases referred have not been adopted yet, we could see that the way the measures we are discussing here is being implemented does not only raise legal doubts from an international point of view, but also from an internal point of view.[38]

II. The EU answers: from the stand-still position towards adequate protection

The nature of the extra-territorial effects of the US decisions have provoked reactions from the EU authorities[39]. We will comment on them in what follows. Nevertheless, we will make first a description of the European and EU legal background in what concerns privacy and personal data protection in order to visualize clearly the legal fundaments of EU concerns. We will also assess which would be the legal basis to regulate on the trans-border data flows (TBDF) under analysis.

Process Clause of the Fifth Amendment of the United States Constitution; (4) Violation of the Right to Travel and Associate Anonymously in Violation of the First and Fifth Amendment of the United States Constitution; (5) Violation of the Right to Petition the Government for Redress of Grievances in Violation of the First Amendment of the United States Constitution; (6) Violation of the Right to Equal Protection in Violation of the Fifth Amendment of the United States Constitution.

[37] E. HASBROUCK "Establishment and Exemption from the Privacy Act of Records System DOT/TSA 010, 'Aviation Security-Screening Records (ASSR)'", 23th February 2003, available at: http://hasbrouck.org/articles/Hasbrouck_DOT_comments-23FEB2003.pdf , last visited 02/09/03.

[38] Pending Bills dealing with CAPPS II have been object of different Amendments issued by members of the US Senate and the US House of Representatives. See: the Wyden Amendment, available at: http://www.epic.org/privacy/airtravel/wyden_capps_amdt.pdf , last visited 02/09/03; the Sabo Amendment, available at: http://www.house.gov/sabo/pr03-18.htm , last visited 02/09/03.

[39] As well as from European civil liberties advocates. See, for instance, the "Campaign against the illegal transfer of European travellers' data to the USA" organised by EDRI (European Digital Rights), information available at: http://www.edri.org/cgi-bin/index?funktion=view&id=000100000085 , last visited 08/08/03.

II.1. European (international level) and EU (supranational level) legal background

When analysing privacy and data protection applicable legislation in Europe we have to consider a plethora of instruments at different levels. It is important to understand their different scope of application as well as their relevance.

In the International context we have to focus on the Council of Europe Convention. Privacy is a fundamental right included in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[40], where it is stated:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

This provision has been largely interpreted by the doctrine, as well as applied by the European Court of Human Rights (ECHR).[41] It is the source for EU legislation dealing with privacy and the protection of personal data, as well as of national legislation. We will come back to the interpretation given by the ECHR to the exception contained in point 2 of the Article, since it is clearly relevant for the topic under study.

The Council of Europe has adopted also the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108[42], and a series

---

[40] Convention for the Protection of Human Rights and Fundamental Freedoms ETS no.: 005, Rome 4/11/50. Available at: http://conventions.coe.int/treaty/en/WhatYouWant.asp?NT=005
D. YERNAULT "L'efficacité de la Convention Européenne des Droits de l'homme pour contester le système 'Echelon' ", in *Sénat et Chambre des Représentants de Belgique*, *Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé 'Echelon'* , 25 Feb. 2002. In this article, the author studies the nature of the ECHR: (1) as an instrument guaranteeing "European public order", considered as a coherent whole, in the sense that it was qualified by the Strasbourg Court in 1995; (2) as an international treaty that gives place to the State's international liability; and (3) as an international treaty of a particular nature, due to its Article 53, by virtue of which adherent States recognise its legal pre-eminence over any other internal or international regulation that would be less protective of Fundamental Rights than the Convention itself.

[41] Case *"Amann v. Switzerland"* (Application n. 27798/95), Strasbourg, 16 February 2000; Case *"Rotaru v. Romania"* (Application n. 28341/95), Strasbourg, 4 May 2000; Case *"P.G. and J.H. v. The United Kingdom"* (Application n. 44787/98), Strasbourg, 25 September 2001, etc.

[42] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no.:108, Strasbourg 28-01-1981. Available at: http://conventions.coe.int/treaty/en/Treaties/Html/108.htm

of Recommendations following a sectoral criteria[43]. We have to bear in mind that this Convention is of great importance for areas that are not covered by Community law, such as those of the second and third pillar, since Directive 95/46/EC[44] is a first pillar Directive, which application is excluded in relation to those areas. Furthermore, most of EU Member States, while transposing the Directive to their internal law, have extended the scope of the national data protection law to the areas excluded by the Directive (e.g. criminal law). In those cases, national law has to respect Convention no. 108. Apart from that, it is important to point out that, whereas if any legal problem arises concerning those areas the European Court of Justice can not intervene, it will be the European Court of Human Rights the one that would give an answer to any case of potential violation to Article 8 at national level.

At EU level, the European Union Charter of Fundamental Rights[45] has included in its scope not only the right to privacy but also the right to the protection of personal data as a distinct fundamental right:

Article 7, Respect for private and family life:

> *"Everyone has the right to respect for his or her private and family life, home and communications".*

Article 8, Protection of personal data:

> *"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".*

Even if, for the time being, the Charter is not legally binding, its philosophy affects the three pillars of EU law. The Charter stresses the nature of privacy and data protection as

---

[43] Among others: Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999); Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997); Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991); Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations (13 September 1990); Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987), etc.

[44] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEC L 281 , 23/11/1995, p. 31 – 50, hereinafter: "the Directive".

[45] Full text of the Charter of fundamental Rights of the European Union, OJEC C 364/1, 18-12-200: http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf. See also: Article 29 Data Protection Working Party, *Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights*, 7th September 1999, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp26en.htm

fundamental rights within the EU and individualize each one, pointing out their autonomy. That proves that they are essential concepts for the EU policy design, and constitute part of European public order.[46]

Beyond Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which mentions only the right to privacy (even if the interpretation has extended it to "data protection"[47]), the EU Charter asserts that data subjects are protected not only as regards their sensitive data or intimacy but also concerning all their personal data (what is, indeed, an objective concept), not only against States' action but also against private bodies. In order to ensure that protection the Charter does emphasise three main principles : 1. the absolute obligation to control the legitimate purposes pursued by the data controller; 2. the right of the data subject to access his own data and 3. the need for an independent authority to intervene in order to control the respect of the two first principles.[48]

Furthermore, the draft Treaty establishing a Constitution for Europe[49] establishes in its Article 50 that :

> *"1. Everyone has the right to the protection of personal data concerning him or her.*
> *2. A European law shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union Institutions, bodies and agencies, and by the Member States when carrying out activities which come under the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of an independent authority".*

II.2. Legal basis to regulate on TBDF

The first aspect to be considered is the legal basis to regulate the transfer of personal data made as a result of the requirements of US authorities, as well as the access to systems located in the EU from the US.

---

[46] See on that point, our reflections published in Y. POULLET, "Pour une justification …", *op.cit.*, p. 240 and ss.

[47] See: L. BYGRAVE "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology*, vol. 6 no. 3. This paper examines the extent to which the basic principles of data protection laws may be read into provisions in human rights treaties proclaiming a right to privacy.

[48] For a more in-depth analysis of the articles 7 and 8 of the Charter and the significance of the distinction between data protection and privacy, Y. POULLET, "Pour une justification …", *op.cit*., p. 277 and 278.

[49] Submitted to the President of the European Council in Rome on 18th July 2003, available at: http://european-convention.eu.int/docs/Treaty/cv00850.en03.pdf , last visited 29/08/03.

II.2.1. Is Directive 95/46/EC applicable to the transfer of passengers' personal data ?

Secondary legislation regulating the protection of privacy and personal data has been adopted in the context of the first pillar of EU law through two Directives: a general Directive 95/46/EC and a specific Directive 97/66/EC[50] concerning the processing of personal data and the protection of privacy in the telecommunications sector (to be replaced by the privacy and electronic communications Directive 2002/58/EC in 31 October 2003)[51].

Indeed, Directive 95/46/EC was passed with the objective of preventing Member States from restricting or prohibiting the free flow of personal data between them for reasons connected with the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. In order to achieve this goal it harmonises, to a certain extent, the rights and obligations in relation to the processing of personal data, creating a high standard of protection for personal data.

It is clear that the general Directive is applicable to the processing of personal data (material scope of application[52]) carried out by airline companies (personal scope of application, being "data controllers"[53]) in the EU (spatial scope of application[54]). Then, if they proceed to transfer this data abroad, consideration has to be given to Articles 25 and 26 of the Directive.

Nevertheless, and given the particular nature of this TBDF, that is, not being made by the companies at their own initiative, but as a consequence of a mandatory requirement imposed by US authorities for the purpose of identifying individuals who may pose a threat to aviation safety or national security[55], we may wonder whether Articles 25 and

[50] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector; OJEC L 024 , 30/01/1998, p. 1 – 8

[51] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJEC No L 201, 31 July 2002. Article 3 §1 states: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". PNR system would not fall under this category. On the scope of application of the new Directive see: S. LOUVEAUX and MV. PEREZ ASINARI "New European Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector. Some initial remarks", *Computers and Telecommunications Law Review*, volume 9, issue 5, 2003, p. 133-138.

[52] Article 3 of the Directive.

[53] Article 2(d) of the Directive.

[54] Article 4.1(a) of the Directive.

[55] We will analyse the "purpose" *infra*.

26 of the Directive would be the proper legal basis to regulate the TBDF in this particular case, or whether it would be the only legal basis to tackle the requirements.

Indeed, assessment would have to be made about the role that the second and/or third pillars (Titles V and VI of the TEU) of EU law would play in this context.

Regarding the second pillar, in Article 11 of the TEU it is stated:

> *"1. The Union shall define and implement a common foreign and security policy covering all areas of foreign and security policy, the objectives of which shall be:*
>
> *-to safeguard the common values, fundamental interests, independence and integrity of the Union in conformity with the principles of the United Nations Charter,*
>
> *-to strengthen the security of the Union in all ways,*
>
> *-to preserve peace and strengthen international security, in accordance with the principles of the United Nations Charter, as well as the principles of the Helsinki Final Act and the objectives of the Paris Charter, including those on external borders,*
>
> *-to promote international cooperation,*
>
> *-to develop and consolidate democracy and the rule of law, and respect for human rights and fundamental freedoms".*

As far as the third pillar is concerned, Article 29 TEU states:

> *"Without prejudice to the powers of the European Community, the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia.*
>
> *That objective shall be achieved by preventing and combating crime, organised or otherwise, in particular terrorism,(...)".*

If for the safeguarding of those objectives it would be considered necessary to enter into an agreement with the US, then, the way to instrument this decision would not be based on a Directive which legal basis is former Article 100A TEC (current Article 95 TCE), being a legal basis for Internal Market instruments.

A very delicate question is then: would an agreement under Articles 24 or 38 TEU, which regulate the conclusion of international agreements when necessary for the

implementation of the respective Titles of the TEU, be necessary? In case of a positive answer, would this exclude the application of the Directive?

In our opinion, the application of the Directive would not be excluded, since the bodies required to send passengers' personal data are private bodies, which processing activities are regulated by this Directive. Even if an agreement under Articles 24 or 38 TEU dealing with the transfer of personal data in the circumstances we are describing in the present article would be situated under the scope of Article 13.1 of the Directive (then processing activities would be legitimated under Article 7(c)), data controllers (airline companies) would not be exempted from all their obligations. We have to bear in mind that Article 13.1 does not exempt data controllers from the respect of Articles 8, 17 and 18 of the Directive. That means that in the field of the airline companies responsibilities, obligations remain *vis-à-vis* the data subject. As a consequence, if they do not comply with those obligations while transferring data they could be declared liable.

Furthermore, since the relationship between the passenger and the airline company is regulated, *prima facie*, by the Directive, and considering that we are dealing with a transfer that will be used in the context of CAPPS II to take "automated individual decisions", attention has to be paid to Article 15 of the Directive, which has not been mentioned in Article 13.1 of the Directive either.

However, and given the intricate characteristics of the situation we are commenting, additional actions would have to be taken, that will exceed the first pillar. Indeed, one may wonder whether the EU can accept that data with EU origin received by US authorities be used, for instance, as part of the evidence in a judicial process that might result in the death penalty[56], or whether "reciprocity"[57] in the case of flights coming to the EU from the US under certain circumstances would be required, etc. Those issues, among others, might be the object of an international agreement based on Articles 24 or 38 TEU[58] that would complement the regulations of Directive 95/46/EC. (Indeed, it seems that the third pillar would have more relevance than the second one in this realm).

[56] In this regard see the Article 13 of the Agreement on extradition between the European Union and the United States of America, OJEC L 181/27, 19.07.2003: "Capital punishment. Where the offence for which extradition is sought is punishable by death under the laws in the requesting State and not punishable by death under the laws in the requested State, the requested State may grant extradition on the condition that the death penalty shall not be imposed on the person sought, or if for procedural reasons such condition cannot be complied with by the requesting State, on condition that the death penalty if imposed shall not be carried out. If the requesting State accepts extradition subject to conditions pursuant to this Article, it shall comply with the conditions. If the requesting State does not accept the conditions, the request for extradition may be denied".

[57] We read in the point (43) of the Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration: "[i]n the event that the European Union decides to adopt an airline passenger identification system similar to that of the US Government, which requires all air carriers and GDSs to provide European authorities with access to PNR data for persons whose current travel itinerary includes a flight to, from, through or within the European Union, CBP and TSA would encourage US based airlines to cooperate".

[58] The Europol Convention has its own regulation on personal data protection, as well as specific rules dealing with TBDF, requiring also "adequacy" in the third country in question.. See article 18 of the Europol Convention adopted by Act of Council on 26 July 1995, OJEC C 316, 27.11.1995. However for

II.2.2. Which TBDF provision is applicable under Directive 95/46/EC ?

Considering that the Directive has to be applied to this case, Article 25.1 of the Directive has to be taken into account, since it sets out the principle that Member States shall only allow a transfer to take place if the third country in question ensures an "adequate" level of protection. The aim of this regulation is protecting data subjects' rights and preventing circumvention of the rules contained in the Directive by sending personal data to countries where the rules are not as strict as in the EU or simply inexistent in order to carry out processing activities[59].

This general principle is softened in different ways by several provisions of the Directive. In the case of passengers' data required by the US it is necessary to analyse what is the suitable legal mechanism to allow this procedure in a lawful way. We have to assess then, which are the derogations to the general principle, what are the characteristics of the US requirements[60], and as a consequence which measures would the EU need to adopt.

The notion of "adequate" protection, though, has to be linked to the degree of risk a transfer presents and to the nature of the data. *"The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country"*[61].

II.2.2.1. Is Article 26.1. applicable ?

There are some cases in which a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection can take place. A set of

---

the transfer of passengers' data, as we have already said, EU public bodies do not intervene. Yet, this Convention was adopted in the context of ex-Article K.3 (current 31 TEU), what reveals that the concept of "adequacy" is neither unknown nor irrelevant in the third pillar sphere.

[59] We have to bear in mind that otherwise, member States would be subject to liability for violation of the ECHR. See on that point, D. YERNAULT "L'efficacité de la Convention Européenne des Droits de l'homme…", *op. cit.*

[60] In fact, this aspect goes beyond TBDF, and consist in an exploration concerning how far the requirements themselves will influence the legal basis: first pillar (Articles 25/26 or 4.1.(c) of the Directive), second pillar, third pillar of EU law. See *infra* for this analysis.

[61] Article 25.2 of the Directive.

derogations to the general principle is created by the Directive, so the transfer will be possible when:

> *"(a) the data subject has given his consent unambiguously to the proposed transfer; or*
> *(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or*
> *(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or*
> *(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or*
> *(e) the transfer is necessary in order to protect the vital interests of the data subject; or*
> *(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case."*[62]

The use of those derogations would not be suitable for the case under analysis.[63] If we consider paragraph (a), for instance, we know that "consent" should be "freely given" (among other characteristics that "consent" should fulfil to be considered valid), and this is not indeed the case here because airline companies are obliged to send the data. Furthermore, even if the relationship between the airline company and the passenger is of purely private order, where party autonomy prevails, a passenger can not agree with a company for something that the company is not free to do or not, and as a consequence, the rules of liability would not be the standard ones, but the exceptional ones (if the US government misuse the data transferred by the airline companies, and given the case that a data subject sue a company, the company will oppose an exception to its liability due to its mandatory public duties (*factum principis*).

If we consider paragraph (d), its application will lead us to the rules contained in Article 13.1 of the Directive. The said regulation provides that :

> *"Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:*
> *(a)national security;*

[62] Article 26.1 of the Directive.

[63] The impossibility to use those derogations in the context of the transfer of travellers' personal data by air companies to the US as a general rule has been clearly explained by the Article 29 Data Protection Working Party. See its *Opinion 6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States*, 24th October 2002, WP 66, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2002.htm

(b)defence;
(c)public security;
(d)the prevention, investigation, detection and prosecution of criminal offences, or breaches of ethic for regulated professions;
(e)an important economic or financial interest of a Member sate or of the European Union, (...);
(f)a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g)the protection of the data subject or of the rights and freedoms of others."[64]

Then, it is required that the exception does not take place in a systematic fashion since exceptions are of restrictive interpretation and application. A hypothetical measure using this Article as legal basis to allow the application of the derogation contained in Article 26.1(d) would not be taken for the "national security" of a Member State, but for the compliance with the requirements of a third country "national security", which does not seem to be the strict fundament for the exception as foreseen in the letter of the EU law. Furthermore, if any exception to the protection of data privacy is adopted respect has to be given to Article 8.2 of the European Convention on Human Rights and Fundamental Freedoms, that is, the restriction must be adopted "in accordance with the law" and when "necessary in a democratic society". Those requisites are, indeed, cumulative[65]. To use this exception a law should be passed (at national or supranational level), and the Member State or the EU would have the burden to prove that there is no other mean to safeguard the public interest at stake in a less-invasive-to-privacy way, or less violating of the data subject' rights.[66]

---

[64] See also Recitals 43, 44, and 45 of the Directive.

[65] "The interference was not therefore 'in accordance with the law' as required by the second paragraph of Article 8 and there has been a violation of this provision. In these circumstances, an examination of the necessity of the interference is no longer required", European Court of Human Rights, case *P.G. and J.H. v. The United Kingdom* (Application n. 44787/98), Strasbourg, 25th September 2001, p. 17. "The Court concludes that the interference cannot therefore be considered to have been 'in accordance with the law' since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration. (...) Having regard to the foregoing conclusion, the Court does not consider it necessary to examine whether the other requirements of paragraph 2 of Article 8 were complied with", European Court of Human Rights, case *Amann v. Switzerland* (Application n. 27798/95), Strasbourg, 16th February 2000, p. 19. See also: Vincent COUSSIRAT-COUSTERE "Article 8 § 2", in *La Convention Européenne des Droits de l'Homme. Commentaire article par article*, Louis PETTITI, Emmanuel DECAUX et Pierre IMBERT (eds), Economica, 2e Edition, Paris, 1999, p. 323-351.

[66] The same debate has been held as regards the exchange of personal data between Europol and the US just after the 11th of September tragic events. After long debate the JHA Council has approved a draft agreement between US and EU on 19th December 2002. On this agreement and certain concerns expressed on its legitimacy, see the report of the EU Network of Independent Experts in Fundamental Rights, "The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats", Thematic Comment drafted upon request of the European Commission, DG Justice and Home Affairs, Unit A5, submitted on 31st March 2003, p. 24, available at: http://www.statewatch.org/news/2003/apr/CFR-CDF.ThemComment1.pdf , last visited 08/08/03.

II.2.2.2. Is Article 26.2. applicable ?

Another alternative way for making a safe transfer is the use of contractual clauses.[67] They can be proposed by the controller (in this case, hypothetically, the airline company) to the member State Authority for approval, they can be elaborated by this Authority as "standard contractual clauses" or even by the European Commission. This is the case of a Commission Decision on standard contractual clauses for the transfer of personal data to third countries (to controllers) under article 26.4 of Directive 95/46/EC [68] and the Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC[69].

However, given the specific circumstances of the case we are dealing with, this is not an appropriate way either, since the transfer of personal data is not being made on the basis of voluntary initiatives taken by the data exporter and the data importer, but rather from an obligation to transfer data arisen from US law that is imposed to airline companies.

II.2.2.3. What about the application of the "Safe Harbour Principles" ?

Apart from the derogations mentioned above, the European Commission may find that a third country ensures an adequate level of protection of personal data and issue a Decision declaring the "adequacy", what will result in the free circulation of data in the circumstances described in the mentioned instrument. Given the remarkable different conception for the protection of personal data and privacy existent in the EU and the US it was not possible for the European Commission, even after long negotiations with US civil servants, to declare that the country regime, as a whole, assures an adequate level of protection. A partial solution was found with the adoption of the Agreement known as "Safe Harbour"[70], which determines that an arrangement put in place by the US Department of Commerce provides adequate level of protection for personal data transferred from the EU. The results are the Safe Harbour principles, which are supplemented by FAQs (Frequently Asked Questions), published by the Department of Commerce.

---

[67] Article 26.2 of the Directive.

[68] Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC - OJEC L 181/19 of 4.7.2001, available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf

[69] Commission Decision 2002/16/EC of 27 December 2001on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC- OJEC L 006 of 10.01.2002, p. 52 – 62, available at:
http://www.europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-16_en.pdf

[70] Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce - OJEC L 215/7 of 25.8.2000.

Adherence to these principles is voluntary, but is only available for companies under the jurisdiction of certain public bodies that control the fairness of "commercial" practices. Indeed, European airline companies[71] are not under the jurisdiction of those bodies.

A specific agreement would be necessary for the transfer of air passengers' data to US authorities. What should be the characteristics of this instrument? What are the main issues at stake? What is the state-of-the-art of the EU-US dialogue in this realm? We will address those issues in the following points. Notwithstanding, it is important to consider that there are other legal issues that need to be taken into account concerning US requirements.

II.2.3. A crucial question : Article 4.1.c) or Article 25.1. ?

Before going further, another relevant issue to discuss is: what kind of system will be/is being implemented by U.S. authorities to gain knowledge of passengers' data? Even if we have been mentioning the fact of "transfers" so far, it has to be noted that "transfer" ("push" system) is required to feed certain data bases such as APIS and that direct "access" to PNR ("pull" system) is also required.

The factual procedure (pull or push) will derive in a different legal regime to be applied. Whereas for the "push" system application of Articles 25 and 26 of the Directive has to be made, the "pull" system will configure the case described in Article 4.1.c) of the Directive, considering the presence of the connecting factor as described in this norm, what would certainly derived in the application of the Directive as a whole.[72]

Article 4.1(c) foresees that the national law transposing the Directive is applicable to the processing of personal data where *"the controller is not established on Community territory and, for the purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for the purposes of transit through the territory of the Community"*.

Can US authorities, accessing PNR data stored in an on-line system situated in the territory of a Member State, be considered as "controller" of this data ? We know that

[71] It has to be noted that not only European airline companies are subject to the Directive 95/46/EC, but every company processing personal data in the EU.

[72] The Article 29 Data Protection Working Party has expressed the same view in this particular issue. See Article 29 Data Protection Working Party, *Opinion 6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States*, 24th October 2002, WP 66, p. 7. Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data*, 13th June 2003, WP 78, p. 7. For a clarification on "applicable law" issues see: Article 29 Data Protection Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, 30 May 2002, WP 56. See also, on the application of Article 4.1(c): MH. BOULANGER and C. de TERWANGNE "Internet et le respect de la vie privée", in *Cahiers du Centre de Recherches Informatique et Droit*, n . 12, 1997, p. 211.

the controller is the person who "determines the purposes and means of the processing data"[73]. We could envisage that the purpose US authorities have for accessing to the PNR (access is a processing activity) be the fight against terrorism, and the means they decided to use for processing passengers' data as one way to fight against terrorism be the PNR system. If the reasoning is made in that direction, that following the letter of the Directive and the interpretation of the Article 29 Data Protection Working Party can certainly be the case, then the controller (the US government), should designate a representative established in the territory of the Member State where the equipment is located (Article 4.2 of the Directive), who should comply with the obligations foreseen in the Directive for data controllers (notification, information, security measures, etc.).

We can see that the Joint Statement, elaborated by the European Commission and US Customs after the Talks on PNR transmission, has incorporated the following wording in point 5.1: "In *accessing* the PNR data in the territory of the Community, US Customs undertakes to respect the principles of the Data Protection Directive"[74]. Nevertheless, we could infer that the actual meaning of this phrase has not been fully considered since there is no evidence of a US will to designate a representative established in the territory of the EU (the relevant Member State) who will comply with the obligations above mentioned. Even if this "will" would exist, who would be the legitimate representative of the US government (who would be responsible in case of non-compliance)?[75] May be, this would be another issue to consider in a third pillar agreement.

After "accessing" to PNR, data will be transferred to the US to be integrated, for instance, into CAPPS II. This transfer will require application of Articles 25 and 26 (it has to be born in mind that, when Article 4.1(c) foresees the application of the Directive as a whole, it does not exclude the rules dealing with TBDF if following the use of equipment in the EU a transfer takes place). Then, an adequacy assessment will have to be made in this regard.

II.2.4. Preliminary conclusions

[73] Article 2(d) of the Directive.

[74] The Annex to the Joint Statement adds that "The United States Customs Service represents that: by legal state (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), air carriers operating passenger flights in foreign air transportation to, from or through the United States, must provide with electronic *access* to PNR data contained in the automated reservation/ departure control systems ('reservation systems')". In the following paragraphs the idea of "access" is reinforced: "with regard to the PNR data which Customs *accesses directly* from the air carrier's reservation systems, Customs will only view PNR data concerning persons whose travel includes a flight into, out of or through the United States; Customs will *access* air reservation systems as an accommodation to the air carriers to obviate the need for costly technical changes required to allow the air carriers to transmit the data to Customs". Italics have been added by the authors.

[75] This is a role that would certainly not be assumed by the US Embassy for reasons of Public International law.

To sum up, we can say that whereas Directive 95/46/EC is applicable to airline companies for regulating the requirements of US authorities regarding access and transfer of passengers' data consideration would have to be given to the need of an agreement between the EU and the US in the field of the second or third pillars of EU law. Concerning the applicability of the Directive, if what is required is "access" to PNR, then Article 4.1(c) and 4.2 are the rules to be taken into account (plus Articles 25 and 26, to cover the transfer to take place subsequently to the access). If, on the contrary, the requirements consist in the "transfer" of data (without direct access), Articles 25 and 26 will play their role. As far as the derogations to Article 25.1 are concerned, the most appropriate of them would be a Decision based on Article 25.6, provided all the requirements for an Adequacy Finding are strictly given.

II.3. Actions undertaken

Quite rapidly after the US decisions concerning passengers' data certain EU Data Protection Commissioners have expressed doubts and concerns about the compliance of the US requests with the EU Data Protection requirements. That lead to the delivery of a first Opinion by the Article 29 Data Protection Working Party taken on its own initiative[76].

More generally, the Working Party has issued a document on the need for a balance approach to the fight against terrorism[77] where it stresses the need for respect all data protection principles in the legislation adopted and also expresses certain concern about the tendency to represent the protection of personal data as a barrier to the efficient fight against terrorism. "The Working Party underlines, in particular, the necessity to take into account the long term impact of urgent policies rapidly implemented or envisaged at this moment. This long-term reflection is all the more necessary in view of the fact that terrorism is not a new phenomenon and cannot be qualified as a temporary phenomenon. The Working Party also underlines the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy as required by Art. 8 of the European Convention on Human Rights and the relevant case-law. This implies *inter alia*, the obligation to demonstrate that any measure taken corresponds to a 'imperative social need'. Measures which are simply 'useful' or 'wished' may not restrict the fundamental rights and freedoms.(…)".

---

[76] Article 29 Data Protection Working Party, *Opinion 6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States*, 24th October 2002, WP 66, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2002.htm

[77] Article 29 Data Protection Working Party, *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism,* 14th December 2001, WP 53, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp53en.pdf
See also: EU Network of Independent Experts in Fundamental Rights, "The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats", Thematic Comment drafted upon request of the European Commission, DG Justice and Home Affairs, Unit A5, submitted on 31st March 2003.

A Joint Statement[78] was signed between the European Commission and US Customs, following high level officials' talks on PNR transmission. Certain undertakings were asked to US authorities in order to comply with the Data Protection Directive. Furthermore, full exercise of the US Freedom of Information Act (FOIA) in connection with the data collected by US authorities in order to provide access to data by EU data subjects, as well as certain limits as regards the transmission of PNR data by the US Customs and TSA to other US administrations were agreed.

Beyond these minimal points of agreement it was explicitly foreseen that other safeguards will be proposed by US through additional undertakings in such a way that adequate protection might be offered to personal data with EU origin and that the European Commission will be able to issue a Decision under Article 25.6 of the Directive.[79]

The validity of the legal basis of this Joint Statement has been seriously challenged by S. Rodota, chairman of the Article 29 Data Protection Working Party, through a letter to the Chair of the EU Parliament's Committee on Citizen's Freedoms and Rights dated 3th March 2003. [80]

The European Parliament has broadly echoed those concerns.[81] A document[82] has been delivered stressing not only the *prima facie* lack of adequate protection offered by the US regulatory system but also denouncing the European Commission's failure, as the guardian of the Treaties and Community law, to assume its responsibilities in full in that "it needs to verify whether there is a real basis in US law to justify access to reservation systems' data or whether this is an over-broad interpretation on the part of the present Administration (…); it is continuing to postpone the verification of the US legislation required under Article 25 of Directive 95/46/EC (…); last but not least, it is failing to provide information to the public, who should be the first to know what is being done with information about them; (…)".[83] It is important to point out that the Parliament,

[78] The Joint Statement has been published on the website of the European Commission (DG External Relations): *European Commission: US Customs talks on PNR transmission*, Joint Statement, Brussels, 17/18 February 2003, available at: http://europa.eu.int/comm/external_relations/us/intro/pnr.htm

[79] At the longer run, both parties agreed on the necessity of a multilateral agreement under the umbrella of International Civil Aviation Organization (ICAO).

[80] The letter recalls that national Data Protection Authorities are not free to apply or not the data protection legislation and "it has not yet been clarified how the Joint Statement might provide a sound legal basis to justify an exception to the rule."

[81] Different hearings have been held by the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. The first one took place on 25th March 2003 ; another one on 6th May 2003.

[82] European Parliament, Motion for a Resolution on transfer of personal data by airlines to the US immigration service, 6th March 2003, B5-0000/2003.

[83] European Parliament, Motion for a Resolution…, p. 3.

despite having regard to Directive 95/46/EC, it expresses being "surprised that these issues have not been considered in the context of the agreements on judicial and police cooperation, (…)", what would let us infer that a double approach (first and third pillar) is being envisaged for the subject matter.

In order to prepare the Commission's Decision under article 25.6 the Article 29 Data Protection Working Party issued a second Opinion on 13th June 2003[84]. This Opinion examines to what extent the US decisions are offering an adequate protection. In what follows we will analyse the principles that should be taken into account when adopting an Adequacy Decision, assessing the way the problems arising in this particular realm are being or should be tackled.

III. Certain considerations for an "adequacy" assessment

This part of the paper does not intend to provide for a complete adequacy assessment for the transfer of passengers' data from the EU to the US. It only points out some specific issues that can present certain problems.

It is clear that the Joint Statement has no legal value,[85] but it is a first step in a dialogue at political level. It does not cover a full analysis of the principles described in the Working Document no. 12 elaborated by the Article 29 Working Party.[86] We will try to make an approximation to the principles described in this Working Document, *vis-à-vis* the Joint Statement and the Undertakings[87] (indeed, the statements made in these documents are related to the "access" to PNR data. We insist on the point that in this case the Directive as a whole has to be applied due to Article 4.1(c)), in the light of the requirements contained in the Aviation and Transportation Security Act, as well as of certain recent documents dealing with CAPPS II.

As we have already mentioned, the Joint Statement says *"(a) [i]n accessing the PNR data in the territory of the Community, US Customs undertakes to respect the principles of the Data Protection Directive"*. The analysis to be made in this regard is what kind of access can be admitted, which part of PNR can be made available to US authorities,

[84] Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data*, 13th June 2003, WP 78, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2003.htm

[85] The sources of Community law are strictly described in Article 249 of the TEC.

[86] Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, 24th July 1998, WP 12, available at:
http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm

[87] Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration, available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78-pnrf-annex_en.pdf

how the Standard Query Language (SGL) will be designed to restrict or filter the access, who will be the representative of the US government in the EU (Article 4.2 of the Directive).

Having said that, and considering that the processing activities to carry out are not only "access" but also "transfer" of the results for further matching at CAPPS II level, respect will have to be given to Articles 25 and 26 of the Directive. Given the analysis we have made *supra*, the appropriate tool for the transfer will be an Adequacy Decision under Article 25.6. The documents reflect a discussion at "adequacy" level, that is, the principles to comply with for an Adequacy Decision, yet there is a complete lack of reference to how compliance with the Directive as a whole will be assured (Articles 4.1(c) and 4.2 of the Directive).

On the other side, the transfer of passengers and crew manifests are not dealt in those documents, whilst it is clear that an "adequacy" assessment and Decision is absolutely necessary in this realm for a legal transfer. In order to structure this adequacy assessment we take as point of departure the three main principles enacted by the EU Charter of Human Rights already evoked:

> *"(…)2.Such data must be processed fairly for specified purposes and on the consent of the person concerned or some legitimate basis laid down by law.2. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".*

- **The legitimate basis and "purpose limitation" principle:**

-The legitimate basis :

According to the Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms a legal and fully transparent legal basis must exist for justifying a data processing limiting privacy rights. This requirement is not fulfilled in the case insofar the US decisions, that is to say the Undertakings, are not at this stage legally binding and that there is no clear view from the European point of view of all the regulations which are surrounding the multiple data processing generated by the PNR flows.

Furthermore, considering that these purposes are determined in a state of "emergency", it would be necessary to add a "sunset clause". Indeed, geopolitical situations[88] can

[88] See the proceedings of the Conference "Les attentats du 11 septembre 2001: Conséquences géopolitiques mondiales et lutte anti-terroriste", Département culturel des Facultés Universitaires Notre-Dame de la Paix de Namur, November 2001.

change very fast, and the purposes for the collection of data that are based in those situations would need to be adapted.

More fundamentally certain doubts might be expressed as regards the requirement of "specificity", which is a hard core principle established by the case law of the European Court of Human Rights[89] grounded on Article 8 of the ECHR. Any extensive exploratory or general surveillance of data[90] is prohibited; the circumstances under which the processing of the data can take place must be specified and the conditions to which it is subject must be identified with sufficient precision.

- the unspecified purpose :

The Joint Statement does not specify the purpose for the transmission of passengers' data. Point 6 states that "[i]t was agreed that the information and undertakings to be provided would need to cover in particular: definition of the purposes for which the data will be used and limitation of the use of these purposes; (…)". Point 5(e) expresses that "US Customs may provide information to other US law enforcement authorities only for purposes of preventing and combating terrorism and other serious criminal offences, who specifically request PNR information from US Customs".

The Annex to the Joint Statement declares that "The United States Customs represents that: (…) PNR data is used by Customs strictly for enforcement purposes, including use in threat analysis to identify and interdict potential terrorists and other threats to national and public security, and to focus Customs resources on high risk concerns, (…)".

The Aviation and Transportation Security Act (ATSA) §114(h)(4) specifies that *"In consultation with the Transportation Security Oversight Board, the Under Secretary shall (...) consider requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals who may pose a threat to aviation safety or national security"*.

There is an urgent need to define the terms used both by US Regulations and the Joint Statement as an answer, not only to the purpose limitation principle contained in European data protection regulations, but more generally to the legality principle of criminal law.

What is "terrorism"?[91] What are the "other serious criminal offences"? What has to be understood by "threat to aviation safety or national security"? How the "potentiality" to

[89] This principle has been constantly repeated by the European Court of Human Rights in what concerns electronic surveillance and wire tapping [see notably recently, *Klass and others v. Germany* (Series A n. 28), Strasbourg 6th September 1978, *Khan v. U.K* (Application n. 35394/97) Strasbourg 12th May 2000]

[90] The European Court of Human Rights has developed its case-law particularly as regards the monitoring of communications, but it seems to us that the same reasoning might be done as regards other data.

[91] It should be clear, before any decision be adopted by EU authorities, which is the definition of "terrorism" and any other relevant concept mentioned as the purposes of US authorities for the processing

be a terrorist will be determined? What kind of parameters will be used? Then, would the purpose of "preventing and combating terrorism and other serious criminal offences" be broadened by the consideration of the purpose expressed in the ATSA? Which other US statute contains purposes for which PNR data or passengers' and crew manifests may be used[92]?

-The "data quality and proportionality" principle:

Data has to be accurate and kept updated. Consideration has to be given, for instance, to the US legislation that determines lists of terrorist groups. Normally, the data on passengers is controlled using those lists. However, the integration of those lists may generate certain concerns. This question has been posed by a Member of the Belgian Parliament in the Hearing organised in June 2001[93].

---

of personal data with EU origin. This issue seems to be problematic even in the EU side: "[n]either international legal instruments, nor the Framework Decision of the Council on 13th June of 2002 concerning the fight against terrorism have really succeed in overcoming the difficulties traditionally encountered when attempting to give a definition of terrorism which describes its specificity, compared to other forms of organized crime in relation to all its possible forms. However, a sufficiently exact definition of the offence of terrorism is a prerequisite not only for specific indictment, but also for the application of specific procedural rules, particularly in the context of the inquiry of the investigation, and even more so for special forms of detention; otherwise the measures adopt in the fighting terrorism will lack clear legal basis, potentially bringing into question their lawfulness". EU Network of Independent Experts in Fundamental Rights, "The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats", Thematic Comment drafted upon request of the European Commission, DG Justice and Home Affaires, Unit A5, submitted on 31st March 2003, p. 7. See the analyses on this specific problem made in pages 11-16. See the definitions given in Articles 1 and 2 by the Framework Decision of 13 June 2002 on combating terrorism, OJCE L 164, 22.6.2002, p.4. See also the Opinion of the Economic and Social Committee on the 'Commission Working Document – The relationship between safeguarding internal security and complying with international protection obligations and instruments', 2002/C 149/09, OJCE C 149, 21.6.2002, specially points 2.7, 2.9, 2.1. A draft global Convention against terrorism is currently being negotiated within the United Nations.

92 Certain concerns might be expressed about the possible use of PNR records for ensuring a better control on immigration (see the possible links with the USVISIT program).

93 "Cependant, il demande si cette loi ne contient pas une certaine forme de rigidité? *[question of a Member of the Parliament in conection to the list of terrorist orgnizations contained in the Antiterrorism and Effective Death Penalty Act of 1996, as described by Mme Sandra Fowler, legal counsel of the Federal Bureau of Investigations –FBI- at the American Embassy]* N'y a-t-il pas un risqué par rapport à des organisations terroristes qui ne seraient pas mentionnées dans cette loi et auxquelles le dispositif ne s'appliquerait pas ? N'y a-t-il pas également des organisations qui disparaissent progressivement ou qui évoluent ? À titre d'exemple, il cite l'OLP, qui, voici quinze ou vingt ans, aurait certainement figuré sur cette liste alors qu'aujourd'hui cette organisation est reconnue comme le représentant du peuple palestinien. Il y a donc des organisations qui ont évolué sur le plan politique et qui ont développe des relations avec les autorités politiques de nos pays", Sénat de Belgique, Session 2000-2001, 2-774/1, Rapport fait au nom de la Commission de l'Intérieur et des Affaires Administratives par M. Wille, II. Auditions d'experts étrangers, 4. Echange de vues, p. 31. On the EU side, lists including persons and entities linked to terrorism are being made. See: Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with the view to combating terrorism, OJEC L 344, 28.12.2001. Article 2.3 states that "The Council, acting by unanimity, shall establish, review and amend the list of persons, groups and entities to which this Regulation applies,

Another concern is expressed by Hasbrouck regarding the quality of the data to be gathered in the context of CAPPS II.[94] Within this system, passengers data will be confronted with data coming from other sources, particularly with the FBI's data base on outstanding warrants for crime and violence. As regards this data base the FBI has explicitly asserted that it has no obligation to ensure the accuracy of the data so processed. Therefore it might happen that a travel would be denied to a person under the basis of a false information.

The exaggerate duration of the data storage has created serious concerns regarding CAPPS II. However, it seems that the doubts have been, to a certain extent, dissipated (see *supra* point I.2). Nevertheless, clarification has to be given regarding APIS.

The principle under analysis is in direct interdependence with the "purpose limitation" one, since whether the data processed is adequate, relevant and not excessive can only be determined in relation to the purpose.

Special attention has to be paid to sensitive data,[95] and the definition given to this concept. For instance, the definition given in the Safe Harbour Agreement differs from the one contained in the Directive. It is expected that in the future Agreement concerning passengers' data respect be given to the definition of he Directive. The Undertakings express that "CBP and TSA are committed to filtering sensitive data (…)".[96] Specifications will have to be given concerning the characteristics of the filters to be implemented or design of SQL.

(…)". This activities will be laid down in accordance with the Article 1(4), (5) and (6) of the Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism, OJEC L 344 , 28.12.2001, where we can read: "4. The list in the Annex shall be drawn up on the basis of precise information or material in the relevant file which indicates that a decision has been taken by a competent authority in respect of the persons, groups and entities concerned, irrespective of whether it concerns the instigation of investigations or prosecution for a terrorist act, an attempt to perpetrate, participate in or facilitate such an act based on serious and credible evidence or clues, or condemnation for such deeds. Persons, groups and entities identified by the Security Council of the United Nations as being related to terrorism and against whom it has ordered sanctions may be included in the list.
For the purposes of this paragraph "competent authority" shall mean a judicial authority, or, where judicial authorities have no competence in the area covered by this paragraph, an equivalent competent authority in that area.
5. The Council shall work to ensure that names of natural or legal persons, groups or entities listed in the Annex have sufficient particulars appended to permit effective identification of specific human beings, legal persons, entities or bodies, thus facilitating the exculpation of those bearing the same or similar names.
6. The names of persons and entities on the list in the Annex shall be reviewed at regular intervals and at least once every six months to ensure that there are grounds for keeping them on the list".
It is not clear then who is the independent authority that monitors that the activities described are carried out with respect of Convention no. 108.

[94] E.HASBROUCK, "What's wrong with CAPPS-II ?", available at : http://hasbrouck.org/articles /CAPPS-II.html , last visited 18/08/03.

[95] Even if the WP n. 12 does not include it in this principle we can certainly connect it with the "proportionality principle".

[96] Undertakings, point (8).

It is further stated that "[w]ith respect to sensitive PNR data that has been transferred by air carriers to CBP, should it become necessary for CBP to use such sensitive data for purposes of preventing and combating terrorism and serious criminal offences, any such use will be subject to specific approval procedures, involving the US Deputy Commissioner of CBP, in consultation with the DHS Chief Privacy Officer".[97] Can the EU accept this statement, considering that if these data has already been transferred, it was made in violation to the Directive?

The proportionality principle assessment, that is whether the data is adequate, relevant and not excessive, has to be complemented by a "necessity test", which normally evaluates to what extent the data kept is the only suitable and available mean for the assurance of the purpose followed. The data is "necessary" if there is no other mean, less invasive, to reach that purpose. The obligation under article 8 of the ECHR to adopt the less privacy intrusive measure has to be recalled in that context.

It is not possible to make a general statement about the implications of the "pull" and the "push" systems because the risks created for the protection of personal data depend on the modalities of implementation of those systems. For instance, it is obvious that if what US authorities require is "full" access to PNR data, this system would be certainly far less respectful of data protection rights than the "transfer" of passengers' and crew manifests, since the amount of data available would be limited in the second case, it would not include sensitive data, etc. However, if we think about the SQL, and the fact that code can be created to determine not only "who" is authorized to access, but also "what" he is entitled to do (only reading, reading and copy, etc) and regarding "which data" (the whole data base, only certain information, about certain persons, etc.), we can see that it can be an interesting way to limit access to sensitive data, or other data considered excessive. Furthermore, it would be possible to check whether unauthorized bodies or persons gain access by analysing the logfiles of the system.

In this regard, it would be also necessary to include a "sunset clause" to evaluate how the limits to the data protection rights created by those systems effectively contribute to the fight against terrorism.

-Restrictions on onward transfers:

The Decision to be adopted by the European Commission should be specific concerning the bodies (public or private) entitled to receive passengers data and the responsibility they have. The Joint Statement is quite vague when saying: "(…) other law enforcement entities may specifically request PNR information from Customs and Customs, in its discretion, may provide such information for national security or in furtherance of other legitimate law enforcement purposes; for purposes of regulating the dissemination of PNR data which may be shared with other law enforcement entities, Customs is

[97] Undertakings, point (9).

considered the 'owner' of the data and such entities are obligated by the terms of disclosure to obtain Customs express authorization for any further dissemination (sometimes referred to as the 'Third Agency Rule'); (…)".

Again, the problem of purpose limitation is present here, "other legitimate law enforcement purposes" is really a very wide purpose that can include any kind of crime, which potentially violates the proportionality principle.

- **The Right to a transparent and secure processing**

-The "transparency" principle:

Passengers have to be provided with information about the purpose of the processing, their rights, as well as which US agencies are entitled to have access to their personal data. The application of this principle can be limited pursuant to Article 13 of the Directive. Any limitation to the right to be informed pursuant to Article 13.1 has to be clearly stated in order to evaluate the proportionality of the measure. Moreover, "[t]he Working Party underlines the necessity to have commitments from the US side that are officially published at least at the level of the Federal Register and fully binding on the US side".[98]

-The "security" principle :

The Annex to the Joint Statement specifies certain characteristics of the security measures. The measures mentioned are those adopted by Customs, but the document is silent concerning the measures adopted by the other bodies to whom data are likely to be transferred/shared with.

-The "rights of access, rectification and opposition":

The Joint Statement affirms that "[a]s concerns a first party request for disclosure of data by the data subject, US Customs will proceed with disclosure under the Freedom of Information Act (FOIA)". It would be advisable to create a standard form for access request under the FOIA with translation to every Community language, considering that not every data subject who travels to the US, and whose data is required in a mandatory way, speaks English, though is able to understand how his rights can be enforced under the FOIA. Translation of the information contained, and to be given as a result of an

[98] Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data*, 13th June 2003, WP 78, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2003.htm

access request, would have to be assured as well, otherwise the data subject who does not speak English will be unable to realize whether he has to exercise his right to rectification or not.

Moreover, the Article 29 Data Protection Working Party[99] has expressed concern about the likelihood of the FOIA being used by third parties to access PNR data held by the US administration. This possibility has to be prevented.

- **Independent authority and enforcement mechanisms :**

There is a lack of clarity concerning what would be the legal remedies available to European data subjects to enforce their rights and obtain redress if necessary. Travelers do not only need to know what are the remedies but also how affordable they are and what kind of assistance they are entitled to receive from public bodies. The system of State liability for misuse of data with EU origin has to be described in the document to be signed.

There is a strong need of an "independent body" to control the respect of the data protection rules regarding EU passengers' data. Indeed, doubts remain concerning the independency of the DHS Chief Privacy Officer.

Conclusions

The Joint Statement and the Undertakings are obviously insufficient to regulate TBDF of passengers' data, both from a formal (they are not a source of Community law) and content (they are far from covering the requirements for an adequacy Decision) point of view.

Concerning the legal basis for EU actions, we reiterate what we have already expressed in the preliminary conclusions, a complementary approach between first and third pillars would have to be developed. Furthermore, whereas "access" should be ruled in the light of Article 4.1.(c) of the Directive, "transfer" has to be ruled under Article 25 and 26. However, an adequacy Decision (Article 25.6) would be required to regulate transfers in both cases (in the case of an integral application of the Directive, as a result of the "transfer" made of "accessed" PNR data).

The way "access" is operated has to be thoroughly described, and limitations must be established concerning the categories of bodies/persons authorized, the categories of data that will be disclosed, and what will be the security measures to be implemented.

[99] Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data*, 13th June 2003, WP 78, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2003.htm

Among others, controls in logfiles will allow to make a follow-up of how "access" is exercised.

The purpose has to be delimited as precisely as possible, since many other parameters of an adequacy assessment have to be regarded *vis-à-vis* this principle (e.g. proportionality, transparency, security, etc.).

We insist on the fact that being the fight against terrorism and the protection to the right of individuals to be safe legitimate purposes, the Directive and the European Convention for the Protection of Human Rights and Fundamental Freedoms give legal instruments to balance the rights to privacy and personal data protection with them. The balance of conflicting rights in accordance to the law (say, respecting the legal parameters to proceed to limit any right) is one of the basis of the democratic system. The conflicting interests have to be interpreted, and the balance has to be made, in conjunction because otherwise contradictory and inapplicable results could arise.

The airline passenger data disclosure case and the EU-US debate

María Verónica Pérez Asinari & Yves Poullet, Centre de Recherches Informatique et Droit (CRID) University of Namur

In the aftermath of the events of 11 September 2001, decisions have been taken unilaterally by US authorities requiring air line companies to provide direct access or transfer of data concerning passengers and cabin crews flying to, from or within the US to certain US administrations. These decisions have been challenged by EU authorities insofar they constitute a violation of EU privacy and personal data protection law which is considered to be of public order. The debate is still pending. This article will comment on this complex and multi-featured discussion opposing two fundamental societal values: on the one hand, the right of the citizens to be protected from terrorism and the obligation of a sovereign State to fight against it and safeguard public security,[1] and on the other hand, the individuals' right to personal data protection and privacy and the obligation of the EU, in the light of international and supranational commitments, to protect them in this arena. After a short presentation of the US decisions and their context, the authors will analyse the EU position, its claim for adequate personal data protection to be ensured by the US authorities and the legal grounds for this position. Finally, a synthetic approach to the adequacy of the US decisions *vis-à-vis* the EU legal provisions will be proposed.

A. The US legal framework

1. The legislative context

Directly after the tragedy of 11 September 2001, the US Government took a great amount of initiatives to fight against terrorism. The Patriot Act,[2] which is commonly known, is one example. However, more specific legislation has been enacted as well, in order to tackle the risks created by the terrorist threat.

In the immigration and admission of aliens sphere, the Enhanced Border Security and Visa Entry Reform Act[3] was enacted on 14 May 2002. As regards air transportation, the US adopted the Aviation and Transportation Security Act (ATSA)[4] on 19 November 2001. This Act has been followed by secondary regulations, notably the document "Passenger and Crew Manifests Required for Passengers Flights in Foreign Air Transportation to the United States", published in the Federal Register on 31 December 2001,[5] and the document "Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States," published in the Federal Register on 25 June 2002.[6]

The main purpose of all this legislation is to enhance security for the fight against terrorism and create what the US authorities have called a "21st Century Smart Border".[7] In order to achieve this goal, the Government and Parliament have given a very large mandate to a new public body: the Transportation Security Agency (TSA), which is part of the Department of Homeland Security,[8] to take appropriate measures in order to improve aviation security.

One of the most important decisions taken in this context was to use information technology, particularly risk analysis tools, for detecting terrorists. All the data transmitted by the air transportation companies will be centralized in a large database, operated both by US Customs and Immigration and Naturalization Services. Furthermore, a Computer Assisted Passenger Pre-screening Program (CAPPS II) is created to evaluate all passengers before they board an aircraft. We will comment more extensively on these initiatives in what follows.

2. The measures

The above referred regulations have created different obligations for air carriers, which derive also in different information management systems, either centralized or not.

The Advanced Passenger Information System (APIS) deals with all the data requested from and transmitted by all air transportation companies. The ATSA stipulates the following:

(1) IN GENERAL - Not later than 60 days after the date of enactment of the Aviation and Transportation Act, each air carrier and foreign air carrier operating a passenger flight in foreign ain transportation to the United States shall provide to the Commissioner of Customs by electronic transmission a passenger and crew manifest

Computer Law & Security Report Vol. 20 no. 2 2004 ISSN 0267 3649/04

containing the information specified in paragraph (2). Carriers may use the advanced passenger information system established under section 431 of the tariff Act of 1930 (19 U.S.C. 1431) to provide the information required by the preceding sentence.

(2) INFORMATION - A passenger and crew manifest for a flight required under paragraph (1) shall contain the following information:

• The full name of each passenger and crew member.

• The date of birth and citizenship of each passenger and crew member.

• The sex of each passenger and crew member.

• The passport number and country of issuance of each passenger and crew member if required for travel.

• The United States visa number or resident alien card number of each passenger and crew member, as applicable.

• Such other information as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety.[9]

Paragraph (4) establishes that the passenger and crew manifest shall be transmitted to the Customs Service in advance of the aircraft landing in the US.[10] Furthermore, the following paragraph regulates on PNR:

(3) PASSENGER NAME RECORDS - The carriers shall make passenger name record information available to Customs Service upon request.[11]

As we have already seen, certain documents have been published in the Federal Register specifying these regulations. The Interim rule of 31 December 2001 has extended the required data elements for the manifests, for instance, by adding the obligation to transmit electronically to Customs:

(3) [t]he foreign airport where each passenger began his air transportation to the United States; for each passenger and crew member destined to the United States, the airport in the United States where the passenger and crew member will process through Customs and Immigration formalities; and for each passenger and crew member transiting through the United States and not clearing through Customs and Immigration formalities, the foreign airport of final destination for the passenger and crew member.[12]

In what concerns PNR, the Interim rule of 25 June 2002 states, among other issues, that:

[i]n order to readily provide Customs with such access to requested PNR data, each air carrier must ensure that its electronic reservation/departure control systems correctly interface with the US Customs data Center, Customs Headquarters.[13]

It is clear then, that these data will not be "transferred" (as a first step, see *infra*) but directly "accessed" on-line.

The Interim rule we are commenting upon further mentions, "merely to be illustrative", certain data elements to which Customs may request access in relation to a passenger:[14]

- Last name; first name; date of birth; address(es); and phone number(s);
- Passenger name record locator (reservation) number;
- Reservation date (or dates, if multiple reservations made), or if no advance reservation made ("go show");
- Travel agency/agent, if applicable;
- Ticket information;
- Form of payment for ticket;
- Itinerary information;
- Carrier information for the flight, including but not limited to: carrier information for each segment of the flight if not continuous; the flight number(s); and date(s) of intended travel;
- Seating; and
- PNR history.[15]

Indeed, PNR data contains other information, some of them of a sensitive nature. PNR, for instance, stores the requested kind of food for the flight (this food can have health, philosophical or religious connotations), whether any facilities for the disabled are needed,[16] etc. It also stores who will pay for the bill (company, association, university, public body, party, etc.) and even in relation to which internal account (what is normally connected to a specific client, project, etc.). The itinerary field includes all air space and related non-airline, auxiliary services the passenger requested.[17]

Another system to be implemented is the US VISIT,[18] which consists of a systematic scanning of the travel documents of each US visitor. Photo and fingerprints will be taken and the data so obtained will be checked against lists of those who should be denied entry within the US territory for different reasons (terrorism, criminal violations, illegal entry, visa violations).[19] This system will permit the central processing of personal data including certain data based on biometric features[20] (today digital photo

PNR data contains other information, some of them of a sensitive nature

and fingerprints; tomorrow facial recognition and iris scans).[21] In order to facilitate this work, visa waiver countries are required to use tamper-proof passports that include biometric identifiers from August 2004. This data will not be requested from airline companies so we will not develop this aspect in the present paper. However, we are of the opinion that its existence had to be mentioned here insofar as US regulations would permit interconnections between the PNR data and the data generated in the context of the US VISIT program.

The TSA is authorized, apart from to use the data collected through these two sources, to establish a "watch-list" of individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety".[22] Furthermore, the different airline companies are operating the Computer Assisted Pre-screening Program (CAPPS), a passenger–screening tool, in order to identify passengers for enhanced screening before their boarding.

An updated version of CAPPS,[23] CAPPS II, is presently being developed for providing a more efficient identification of terrorist risks:

Essentially, CAPPS II process will be a passive system that produces a general indication of the level of terrorist risk each airline passenger might pose to civil aviation security. It will be activated by a traveller's airline reservation request. Airlines will ask passengers for specific reservation information that will include passenger's full name, plus other identifiers including date of birth, home address and home phone number. Passengers will not be asked to provide social security numbers, and TSA will not look at credit worthiness. The CAPPS II process will then authenticate each passenger's identity through publicly and commercially available databases. Once a passenger's identity is authenticated and the passenger's information is run against terrorist or appropriate Federal Government systems, an aggregate numerical threat score will be generated that TSA will use to determine which passengers should proceed through the ordinary screening process and which passengers should be asked to a somewhat more thorough screening. In extremely rare cases, the system may identify an individual who is a known foreign terrorist or the associate of a known foreign terrorist. In such a case, law enforcement authorities would be notified and given the opportunity to take appropriate action.[24]

All these systems will be operated under the control of the TSA. Privacy issues are not absent of the implementation of all these systems. The administrator of the TSA, James M. Loy, said that the TSA is taking privacy issues into account as it develops CAPPS II:

CAPPS II will operate under a stringent privacy protection protocol being developed through discussions with privacy groups (…). Strict firewalls and access rules will protect a traveller's information from inappropriate use, sharing, or disclosure.[25]

According to the ATSA requirement, a Privacy Officer has been nominated in the US Department of Homeland Security[26] to implement privacy requirements and to control their respect. This Privacy Officer is member of the Department of Homeland Security.

It is quite obvious that all the measures described affect significantly data controllers[27] which are operating from foreign countries and create new risks for the protection of personal data with European origin. The data relates to travellers (more or less 12 million passengers) flying to US and the requirements of US government interfere with the national legislation applicable to airline companies' data processing activities in the foreign countries where the passengers make the reservation, buy the ticket, take the plane, etc. and put into question their sovereignty by operating far beyond the US borders. To justify this extraterritorial approach, US authorities have developed a new conception of their own sovereignty not limited to the physical borders:

[b]ut in the 21st Century, border security can no longer be just a coastline, or a line on the ground between two nations. It's also a line of information in a computer, telling us who is in the country, for how long, and for what reason… In the 21st Century it is not enough to place inspectors at our ports of entry to monitor the flow of goods and people. We must also have a 'virtual border' that operates far beyond the land border of the United States.[28]

This reasoning has been also held in the context of the ECHELON case,[29] which is a UK-US system of electronic surveillance of the messages exchanged through satellites. The ECHELON system was, indeed, criticised by the European Parliament as violating the European fundamental right to privacy.[30] (see p 92 above)

Notwithstanding, the TSA issued a notice narrowing the scope of the CAPPS II, published on the Federal Register on 1 August 2003.[31] This notice describes how the TSA will use CAPPS II and which

changes have been made from the notice published at the Federal Register on 15 January 2003. Indeed, many comments and negative reactions were received in response to the prior Privacy Act notice. That has generated an obvious need to make some reforms in the proposal to make it data privacy compliant. For instance, whereas the original document on CAPPS II stated that information about individuals would be maintained for up to 50 years, the new notice expressed that for almost all passengers, that information will be deleted soon after the trip is safely completed, and for a "few risk" persons, the length of time the information will be kept is still under consideration.

3. Reactions in the US

Jan Adams and Rebecca Gordon of California, for example, were detained at San Francisco International Airport, and told that their names appeared on the secret 'no-fly' list. The two women – peace activists who publish a newspaper called War Times – were told nothing about why they were on such a list, or how they could get off. The ACLU has filed suit against the Federal Government on their behalf to find out how the 'no fly' lists were created, how they are being maintained or corrected and, most importantly, how people who are mistakenly included on the list can have their names taken off. One question we believe needs answering is whether our clients are on the 'no fly' list because of their First Amendment protected political views.[32]

This is just an example of the role that civil liberties advocates are playing in the discussion on the implementation of the new measures. The Electronic Privacy Information Center (EPIC) had posted on its website several pages[33] with news about the debate on passenger data and the campaigns against the US policy. Moreover, they have submitted an action against the Department of Homeland Security, the Transportation Security Administration and the Department of Defense, under the Freedom of Information Act (FOIA), seeking the release of agency records concerning airline passenger screening procedures requested by EPIC from defendants.[34]

Indeed, EPIC sent a letter to the TSA on 10 March 2003 requesting records related to CAPPS II project addressing the following subjects:

(a) any existing legal, statutory and/or regulatory frameworks concerning governmental access to and use of transactional and other records about individuals. This request includes, but is not limited to, any assessments of the legal authority (or lack thereof) for information collection activities planned or proposed for the CAPPS II project; and (b) potential privacy and/or civil liberties implications of the activities planned or proposed for the CAPPS II project.

The answer was delivered late and incomplete.

Apart from that, John Gilmore, a US citizen, filed a lawsuit against John Ashcroft (in his official capacity as Attorney General of the US) and other civil servants (with responsibilities in connected areas). Giving a frame to his action he said that he was "concerned that the climate of fear that currently pervades American society [is] eroding long-standing constitutional rights".[35] Basically, he challenged the "secret" character of a regulation limiting people's right to travel anonymously and the use of "no-fly lists" that are created and maintained without transparency and control. In his complaint it is expressed:

[p]laintiff objects to the unregulated use of such lists because he believes history teaches that granting the government unlimited control over 'enemies list' will inevitably result in abuse.

It is interesting to see the myriad of constitutional causes of action raised by the plaintiff.[36] Particularly in what concerns the First Amendment, it has been pointed out that:

[f]ew activities implicate the assembly clause of the First Amendment as directly as travel. When people travel to assemble, as they do when they travel for business or organization meetings or conventions, or to meet friends and relatives, their travel is an act of assembly. Travel is not just an activity often engaged in for purposes protected under other clauses of the First Amendment (such as travel to petition the government for a redress of grievances, or travel for purposes protected as freedom of speech or of the press), but travel is, in and of itself, an activity directly protected under the assembly clause of the First Amendment.[37]

Even if the final decisions of the cases referred have not been adopted yet, we can see that the way the measures we are discussing here are being implemented not only raise legal doubts from an international point of view, but from an internal point of view as well.[38]

B. The EU answers: from the stand-still position towards adequate protection

The nature of the extra-territorial effects of US decisions have provoked reactions from the EU

Travel is, in and of itself, an activity directly protected under the assembly clause of the First Amendment

authorities.[39] We will comment on them in what follows. Nevertheless, we will first describe the European and EU legal background concerning privacy and personal data protection in order to visualize clearly the legal fundamentals of EU concerns. We will also assess what would be the legal basis for regulation of the trans-border data flows (TBDF) under analysis.

1. European (international level) and EU (supranational level) legal background

When analysing privacy and data protection applicable legislation in Europe we have to consider a plethora of instruments at different levels. It is important to understand their different scope of application as well as their relevance.

In the International context we have to focus on the Council of Europe Convention. Privacy is a fundamental right included in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms,[40] where it is stated:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This provision has been largely interpreted by the doctrine, as well as applied by the European Court of Human Rights (ECHR).[41] It is the source for EU legislation dealing with privacy and the protection of personal data, as well as of national legislation. We will come back to the interpretation given by the ECHR to the exception contained in point 2 of the Article, since it is clearly relevant for the topic under study.

The Council of Europe has adopted also the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*,[42] and a series of Recommendations following a sectoral criteria.[43] We have to bear in mind that this Convention is of great importance for areas that are not covered by Community law, such as those of the second and third pillar, since Directive 95/46/EC[44] is a first pillar Directive, which application is excluded in relation to those areas. Furthermore, most of EU Member States, while transposing the Directive to their internal law, have extended the scope of the national data protection law to the areas excluded by the Directive (e.g. criminal law). In those cases, national law has to respect Convention no. 108. Apart from that, it is important to point out that, if any legal problem arises concerning those areas where the European Court of Justice cannot intervene, it will be the European Court of Human Rights that will give a decision on any case of potential violation to Article 8 at national level.

At EU level, the *European Union Charter of Fundamental Rights*[45] has included in its scope not only the right to privacy but also the right to the protection of personal data as a distinct fundamental right:

Article 7, Respect for private and family life:

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8, Protection of personal data:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Even if, for the time being, the Charter is not legally binding, its philosophy affects the three pillars of EU law. The Charter stresses the nature of privacy and data protection as fundamental rights within the EU and individualizes each one, pointing out their autonomy. That proves that they are essential concepts for the EU policy design, and constitute part of European public order.[46]

Beyond Article 8 of the *European Convention for the Protection of Human Rights* and Fundamental Freedoms, which mentions only the right to privacy (even if the interpretation has extended it to "data protection"),[47] the EU Charter asserts that data subjects are protected not only as regards their sensitive data or intimacy but also concerning all their personal data (what is, indeed, an objective concept), not only against States' action but also against private bodies. In order to ensure that protection, the Charter does emphasise three main principles:

1. The absolute obligation to control the legitimate purposes pursued by the data controller;

2. The right of the data subject to access his own data and

3. The need for an independent authority to intervene in order to secure respect for the two first principles.[48]

Furthermore, the draft Treaty establishing a Constitution for Europe[49] establishes in its Article 50 that:

1. Everyone has the right to the protection of personal data concerning him or her.

2. A European law shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union Institutions, bodies and agencies, and by the Member States when carrying out activities which come under the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of an independent authority.

2. Legal basis to regulate on TBDF

The first aspect to be considered is the legal basis to regulate the transfer of personal data made as a result of the requirements of US authorities, as well as the access to systems located in the EU from the US.

(a) Is Directive 95/46/EC applicable to the transfer of passengers' personal data?

Secondary legislation regulating the protection of privacy and personal data has been adopted in the context of the first pillar of EU law through two Directives: a general Directive 95/46/EC and a specific Directive 97/66/EC[50] concerning the processing of personal data and the protection of privacy in the telecommunications sector (replaced by the *Privacy and Electronic Communications Directive 2002/58/EC* on 31 October 2003).[51]

Indeed, Directive 95/46/EC was passed with the objective of preventing Member States from restricting or prohibiting the free flow of personal data between them for reasons connected with the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. In order to achieve this goal it harmonises, to a certain extent, the rights and obligations in relation to the processing of personal data, creating a high standard of protection for personal data.

It is clear that the general Directive is applicable to the processing of personal data (material scope of application)[52] carried out by airline companies (personal scope of application, being "data controllers")[53] in the EU (spatial scope of application).[54] Then, if they proceed to transfer this data abroad, consideration has to be given to Articles 25 and 26 of the Directive.

Nevertheless, and given the particular nature of this TBDF, that is, not being made by the companies at their own initiative, but as a consequence of a mandatory requirement imposed by US authorities for the purpose of identifying individuals who may pose a threat to aviation safety or national security,[55] we may wonder whether Articles 25 and 26 of the Directive would be the proper legal basis to regulate the TBDF in this particular case, or whether it would be the only legal basis to tackle the requirements.

Indeed, assessment would have to be made about the role that the second and/or third pillars (Titles V and VI of the TEU) of EU law would play in this context. Regarding the second pillar, in Article 11 of the TEU it is stated:

1. The Union shall define and implement a common foreign and security policy covering all areas of foreign and security policy, the objectives of which shall be:

• to safeguard the common values, fundamental interests, independence and integrity of the Union in conformity with the principles of the United Nations Charter,

• to strengthen the security of the Union in all ways,

• to preserve peace and strengthen international security, in accordance with the principles of the United Nations Charter, as well as the principles of the Helsinki Final Act and the objectives of the Paris Charter, including those on external borders,

• to promote international cooperation,

• to develop and consolidate democracy and the rule of law, and respect for human rights and fundamental freedoms.

As far as the third pillar is concerned, Article 29 TEU states:

Without prejudice to the powers of the European Community, the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia.

It is clear that the general Directive is applicable to the processing of personal data carried out by airline companies

That objective shall be achieved by preventing and combating crime, organised or otherwise, in particular terrorism, (...).

If for the purpose of safeguarding those objectives it is considered necessary to enter into an agreement with the US, then the way to instrument this decision would not be based on a Directive in which the legal basis is the former Article 100A TEC (current Article 95 TCE), being the legal basis for Internal Market instruments.

A very delicate question is then: would an agreement under Articles 24 or 38 TEU, which regulate the conclusion of international agreements when necessary for the implementation of the respective Titles of the TEU, be necessary? In case of a positive answer, would this exclude the application of the Directive?

In our opinion, the application of the Directive would not be excluded, since the bodies required to send passengers' personal data are private bodies, which processing activities are regulated by this Directive. Even if an agreement under Articles 24 or 38 TEU dealing with the transfer of personal data in the circumstances we are describing in the present article would be situated under the scope of Article 13.1 of the Directive (then processing activities would be legitimated under Article 7(c)), data controllers (airline companies) would not be exempted from all their obligations. We have to bear in mind that Article 13.1 does not exempt data controllers from the respect of Articles 8, 17 and 18 of the Directive. That means that in the field of the airline companies' responsibilities, obligations remain *vis-à-vis* the data subject. As a consequence, if they do not comply with those obligations while transferring data they could be declared liable.

Furthermore, since the relationship between the passenger and the airline company is regulated, *prima facie*, by the Directive, and considering that we are dealing with a transfer that will be used in the context of CAPPS II to take "automated individual decisions", attention has to be paid to Article 15 of the Directive, which has not been mentioned in Article 13.1 of the Directive either.

However, and given the intricate characteristics of the situation we are commenting, additional actions would have to be taken that will exceed the first pillar. Indeed, one may wonder whether the EU can accept that data with an EU origin received by US authorities might be used, for instance, as part of the evidence in a judicial process that might result in the death penalty,[56] or whether "reciprocity"[57] in the case of flights coming to the EU from the US would under certain circumstances, be required, etc. Those issues, among others, might be the object of an international agreement based on Articles 24 or 38 TEU[58] that would complement the regulations of Directive 95/46/EC. (Indeed, it seems that the third pillar would have more relevance than the second one in this realm.)

(b) Which TBDF provision is applicable under Directive 95/46/EC?

Considering that the Directive has to be applied to this case, Article 25.1 of the Directive has to be taken into account, since it sets out the principle that Member States shall only allow a transfer to take place if the third country in question ensures an "adequate" level of protection. The aim of this regulation is protecting data subjects' rights and preventing circumvention of the rules contained in the Directive by sending personal data to countries where the rules are not as strict as in the EU or simply inexistent in order to carry out processing activities.[59]

This general principle is softened in different ways by several provisions of the Directive. In the case of passengers' data required by the US it is necessary to analyse what is the suitable legal mechanism to allow this procedure in a lawful way. We have to assess then, which are the derogations to the general principle, what are the characteristics of the US requirements,[60] and as a consequence which measures the EU would need to adopt.

The notion of "adequate" protection, though, has to be linked to the degree of risk a transfer presents and to the nature of the data.

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[61]

(i) Is Article 26.1.applicable?

There are some cases in which a transfer or a set of transfers of personal data to a third country does not ensure an adequate level of protection. A set of derogations to the general principle is created by the Directive, so the transfer will be possible when:

(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.[62]

The use of those derogations would not be suitable for the case under analysis.[63] If we consider paragraph (a), for instance, we know that "consent" should be "freely given" (among other characteristics that "consent" should fulfil to be considered valid), and this is not indeed the case here because airline companies are obliged to send the data. Furthermore, even if the relationship between the airline company and the passenger is of purely private nature, where party autonomy prevails, a passenger cannot give consent for something that the company is not free to do. As a consequence, the rules of liability would not be the standard ones, but the exceptional ones (if the US government misuses the data transferred by the airline companies, and given the case that a data subject sues the company, the company will oppose an exception to its liability due to its mandatory public duties (*factum principis*).

If we consider paragraph (d), its application will lead us to the rules contained in Article 13.1 of the Directive. The said regulation provides that:

Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or breaches of ethic for regulated professions;

(e) an important economic or financial interest of a Member sate or of the European Union, (...);

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.[64]

It is noted that the exception does not operate in a systematic fashion since exceptions are of restrictive interpretation and application. A hypothetical measure, using this Article as the legal basis to allow the application of the derogation contained in Article 26.1(d), would not be taken for the "national security" of a Member State, but in compliance with the requirements of a third country's "national security". This does not seem to be the strict *raison d'être* for the exception as foreseen in the letter of the EU law. Furthermore, if any exception to the protection of data privacy is adopted respect has to be given to Article 8.2 of the *European Convention on Human Rights and Fundamental Freedoms*, that is, the restriction must be adopted "in accordance with the law" and when "necessary in a democratic society". Those requisites are, indeed, cumulative.[65] To use this exception, a law should be passed (at national or supranational level) and the Member State or the EU would have the burden to prove that there was no other means to safeguard the public interest at stake in a 'less-invasive-to-privacy' way, or less violating of the data subject' rights.[66]

(ii) Is Article 26.2. applicable?

Another alternative way for making a safe transfer is the use of contractual clauses.[67] They can be proposed by the controller (in this case, hypothetically, the airline company) to the member State Authority for approval, they can be elaborated by this Authority as "standard contractual clauses" or even by the European Commission. This is the case of a *Commission Decision on standard contractual clauses for the transfer of personal data to third countries* (to controllers) under article 26.4 of Directive 95/46/EC [68] and the *Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries*, under Directive 95/46/EC.[69]

However, given the specific circumstances of the case we are dealing with, this is not an

There are some cases in which a transfer or a set of transfers of personal data to a third country does not ensure an adequate level of protection

appropriate way either, since the transfer of personal data are not being made on the basis of voluntary initiatives taken by the data exporter and the data importer, but rather from an obligation to transfer data arisen from US law that is imposed upon airline companies.

(iii) What about the application of the "Safe Harbour Principles"?

Apart from the derogations mentioned above, the European Commission may find that a third country ensures an adequate level of protection of personal data and issue a Decision declaring the "adequacy", what will result in the free circulation of data in the circumstances described in the mentioned instrument. Given the remarkably different conception for the protection of personal data and privacy existent in the EU and the US, it was not possible for the European Commission, even after long negotiations with US, civil servants, to declare that the country's regime, as a whole, assured an adequate level of protection. A partial solution was found with the adoption of the Agreement known as "Safe Harbour",[70] which determines that an arrangement put in place by the US Department of Commerce provides adequate level of protection for personal data transferred from the EU. The results are the Safe Harbour principles, which are supplemented by FAQs (Frequently Asked Questions), published by the Department of Commerce.

Adherence to these principles is voluntary, but is only available for companies under the jurisdiction of certain public bodies that control the fairness of "commercial" practices. Indeed, European airline companies[71] are not under the jurisdiction of those bodies.

A specific agreement would be necessary for the transfer of air passengers' data to US authorities. What should be the characteristics of this instrument? What are the main issues at stake? What is the state-of-the-art of the EU-US dialogue in this realm? We will address those issues in the following points. Notwithstanding, it is important to consider that there are other legal issues that need to be taken into account concerning US requirements.

(c) A crucial question: Article 4.1.c) or Article 25.1?

Before going further, another relevant issue to discuss is: what kind of system will be/is being implemented by US authorities to gain knowledge of passengers' data? Even if we have been mentioning the fact of "transfers" so far, it has to be noted that "transfer" ("push" system) is required to feed certain databases such as APIS and that direct "access" to PNR ("pull" system) is also required.

The factual procedure (pull or push) will each derive in a different legal regime. For the "push" system application of Articles 25 and 26 of the Directive has to be made, whereas the "pull" system will configure the case described in Article 4.1.c) of the Directive (considering the presence of the connecting factor as described in this norm, would certainly derive from the application of the Directive as a whole.)[72]

Article 4.1(c) foresees that the national law transposing the Directive is applicable to the processing of personal data where:

The controller is not established on Community territory and, for the purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for the purposes of transit through the territory of the Community.

Can US authorities, accessing PNR data stored in an on-line system situated in the territory of a Member State, be considered as the "controller" of this data? We know that the controller is the person who "determines the purposes and means of the processing data".[73] We could envisage that the purpose US authorities have for accessing the PNR (access is a processing activity) would be the fight against terrorism, and the means they decided to use for processing passengers' data as one way to fight against terrorism would be the PNR system. If the reasoning is made in that direction, following the letter of the Directive and the interpretation of the Article 29 Data Protection Working Party, then the controller (the US government) should designate a representative established in the territory of the Member State where the equipment is located (Article 4.2 of the Directive), who should comply with the obligations foreseen in the Directive for data controllers (notification, information, security measures, etc.).

We can see that the Joint Statement, elaborated by the European Commission and US Customs after the Talks on PNR transmission, has incorporated the following wording in point 5.1:

In accessing the PNR data in the territory of the Community, US Customs undertakes to respect the principles of the Data Protection Directive.[74]

Nevertheless, we could infer that the actual meaning of this phrase has not been fully considered

since there is no evidence of a US will to designate a representative established in the territory of the EU (the relevant Member State) who will comply with the obligations above mentioned. Even if this "will" would exist, who would be the legitimate representative of the US government (who would be responsible in case of non-compliance)?[75] May be, this would be another issue to consider in a third pillar agreement.

After "accessing" the PNR, data will be transferred to the US to be integrated, for instance, into CAPPS II. This transfer will require application of Articles 25 and 26 (it has to be borne in mind that, when Article 4.1(c) foresees the application of the Directive as a whole, it does not exclude the rules dealing with TBDF if, following the use of equipment in the EU, a transfer takes place). Then, an adequacy assessment will have to be made in this regard.

(d) Preliminary conclusions

To sum up we can say that, whereas Directive 95/46/EC is applicable to airline companies for regulating the requirements of US authorities regarding access and transfer of passengers' data, consideration would have to be given to the need for an agreement between the EU and the US in the field of the second or third pillars of EU law. Concerning the applicability of the Directive, if what is required is "access" to PNR, then Article 4.1(c) and 4.2 are the rules to be taken into account (plus Articles 25 and 26, to cover the transfer to take place subsequently to the access). If, on the contrary, the requirements consist in the "transfer" of data (without direct access), Articles 25 and 26 will play their role. As far as the derogations to Article 25.1 are concerned, the most appropriate of them would be a Decision based on Article 25.6, provided all the requirements for an Adequacy Finding are strictly given.

3. Actions undertaken

Soon after the US decisions concerning passengers' data certain EU Data Protection Commissioners expressed doubts and concerns about the compliance of the US requests with the EU Data Protection requirements. That led to the delivery of a first Opinion by the Article 29 Data Protection Working Party taken on its own initiative.[76]

More generally, the Working Party has issued a document on the need for a balance approach to the fight against terrorism[77] where it stresses the need to respect all data protection principles in the legislation adopted and also expresses certain concern about the tendency to represent the protection of personal data as a barrier to the efficient fight against terrorism: The Working Party underlines, in particular, the necessity to take into account the long term impact of urgent policies rapidly implemented or envisaged at this moment. This long-term reflection is all the more necessary in view of the fact that terrorism is not a new phenomenon and cannot be qualified as a temporary phenomenon. The Working Party also underlines the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy as required by Article 8 of the *European Convention on Human Rights* and the relevant case-law. This implies, *inter alia*, the obligation to demonstrate that any measure taken corresponds to an 'imperative social need'. Measures which are simply 'useful' or 'wished' may not restrict the fundamental rights and freedoms. (…).

The Working Party underlines the obligation to respect the principle of proportionality in relation to any measure

A Joint Statement[78] was signed between the European Commission and US Customs, following high level officials' talks on PNR transmission. Certain undertakings were asked of US authorities in order to comply with the Data Protection Directive. Furthermore, full exercise of the US Freedom of Information Act (FOIA) in connection with the data collected by US authorities in order to provide access to data by EU data subjects, as well as certain limits as regards the transmission of PNR data by the US Customs and TSA to other US administrations were agreed.

Beyond these minimal points of agreement it was explicitly foreseen that other safeguards would be proposed by the US through additional undertakings in such a way that adequate protection might be offered to personal data with an EU origin and that the European Commission would be able to issue a Decision under Article 25.6 of the Directive.[79]

The validity of the legal basis of this Joint Statement has been seriously challenged by S. Rodota, chairman of the Article 29 Data Protection Working Party, through a letter to the Chair of the EU Parliament's Committee on Citizen's Freedoms and Rights dated 3 March 2003. [80]

The European Parliament has broadly echoed those concerns.[81] A document[82] has been delivered stressing not only the *prima facie* lack of adequate protection offered by the US regulatory system but also denouncing the European Commission's failure, as the guardian of the Treaties and Community law, to assume its responsibilities in full in that:

it needs to verify whether there is a real basis in US law to justify access to reservation systems' data or whether this is an over-broad interpretation on the part of the present Administration (…); it is continuing to postpone the verification of the US legislation required under Article 25 of Directive 95/46/EC (…); last but not least, it is failing to provide information to the public, who should be the first to know what is being done with information about them; (…).[83]

It is important to point out that the Parliament, despite having regard to Directive 95/46/EC, expresses itself as being "surprised that these issues have not been considered in the context of the agreements on judicial and police cooperation, (…)", which would let us infer that a double approach (first and third pillar) is being envisaged for the subject matter.

In order to prepare the Commission's Decision under article 25.6, the Article 29 Data Protection Working Party issued a second Opinion on 13 June 2003.[84] This Opinion examines to what extent the US decisions are offering an adequate protection. In what follows we will analyse the principles that should be taken into account when adopting an Adequacy Decision, assessing the way the problems arising in this particular realm are being or should be tackled.

C. Certain considerations for an "adequacy" assessment

This part of the article does not intend to provide a complete adequacy assessment for the transfer of passengers' data from the EU to the US. It only points out some specific issues that can present certain problems.

It is clear that the Joint Statement has no legal value,[85] but it is a first step in a dialogue at political level. It does not cover a full analysis of the principles described in the Working Document no. 12 elaborated by the Article 29 Working Party.[86] We will try to make an approximation to the principles described in this Working Document, *vis-à-vis* the Joint Statement and the Undertakings[87] (indeed, the statements made in these documents are related to the "access" to PNR data. We insist on the point that in this case the Directive as a whole has to be applied due to Article 4.1(c)), in the light of the requirements contained in the Aviation and Transportation Security Act, as well as of certain recent documents dealing with CAPPS II.

As we have already mentioned, the Joint Statement says:

(a) [i]n accessing the PNR data in the territory of the Community, US Customs undertakes to respect the principles of the Data Protection Directive.

The analysis to be made in this regard is what kind of access can be admitted, which part of PNR can be made available to US authorities, how the Standard Query Language (SQL) will be designed to restrict or filter the access, who will be the representative of the US government in the EU (Article 4.2 of the Directive)?

Having said that, and considering that the processing activities to carry out are not only "access" but also "transfer" of the results for further matching at CAPPS II level, respect will have to be given to Articles 25 and 26 of the Directive. Given the analysis we have made *supra*, the appropriate tool for the transfer will be an Adequacy Decision under Article 25.6. The documents reflect a discussion at "adequacy" level that is, the principles to be complied with for an Adequacy Decision. Yet there is a complete lack of reference as to how compliance with the Directive as a whole will be assured (Articles 4.1(c) and 4.2 of the Directive).

On the other side, the transfer of passengers and crew manifests are not dealt in those documents, whilst it is clear that an "adequacy" assessment and Decision is absolutely necessary in this realm for a legal transfer to take place. In order to structure this adequacy assessment we take as the point of departure the three main principles enacted by the EU Charter of Human Rights already evoked:

(…)1. Such data must be processed fairly for specified purposes and on the consent of the person concerned or some legitimate basis laid down by law.

2. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

1. The legitimate basis and "purpose limitation" principle:

(a) The legitimate basis:

According to the Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms* a legal and fully transparent legal basis must exist for justifying a data processing limiting privacy rights. This requirement is not fulfilled in the case insofar as the US decisions, that is to say the Undertakings, are not at this stage legally binding and that there is no

clear view from the European point of view of all the regulations which are surrounding the multiple data processing generated by the PNR flows.

Furthermore, considering that these purposes are determined in a state of "emergency", it would be necessary to add a "sunset clause". Indeed, geopolitical situations[88] can change very fast, and the purposes for the collection of data that are based in those situations would need to be adapted.

More fundamentally certain doubts might be expressed as regards the requirement of "specificity", which is a hard core principle established by the case law of the European Court of Human Rights[89] grounded on Article 8 of the ECHR. Any extensive exploratory or general surveillance of data[90] is prohibited; the circumstances under which the processing of the data can take place must be specified and the conditions to which it is subject must be identified with sufficient precision.

(b) The unspecified purpose:

The Joint Statement does not specify the purpose for the transmission of passengers' data. Point 6 states that:

[i]t was agreed that the information and undertakings to be provided would need to cover in particular: definition of the purposes for which the data will be used and limitation of the use of these purposes; (…)". Point 5(e) expresses that "US Customs may provide information to other US law enforcement authorities only for purposes of preventing and combating terrorism and other serious criminal offences, who specifically request PNR information from US Customs.

The Annex to the Joint Statement declares that:

The United States Customs represents that: (…) PNR data is used by Customs strictly for enforcement purposes, including use in threat analysis to identify and interdict potential terrorists and other threats to national and public security, and to focus Customs resources on high risk concerns, (…).

The Aviation and Transportation Security Act (ATSA) §114(h) (4) specifies that:

In consultation with the Transportation Security Oversight Board, the Under Secretary shall (…) consider requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals who may pose a threat to aviation safety or national security.

There is an urgent need to define the terms used both by US Regulations and the Joint Statement as an answer, not only to the purpose limitation principle contained in European data protection regulations, but more generally to the legality principle of criminal law.

What is "terrorism"?[91] What are the "other serious criminal offences"? What has to be understood by "threat to aviation safety or national security"? How is the "potential" to be a terrorist be determined? What kind of parameters will be used? Then, would the purpose of "preventing and combating terrorism and other serious criminal offences" be broadened by the consideration of the purpose expressed in the ATSA? Which other US statute contains purposes for which PNR data or passengers' and crew manifests may be used?[92]

(c) The "data quality and proportionality" principle:

Data has to be accurate and kept updated. Consideration has to be given, for instance, to the US legislation that determines lists of terrorist groups. Normally, the data on passengers is controlled using those lists. However, the integration of those lists may generate certain concerns. This question has been posed by a Member of the Belgian Parliament in the Hearing organised in June 2001.[93]

Another concern is expressed by Hasbrouck regarding the quality of the data to be gathered in the context of CAPPS II.[94] Within this system, passengers' data will be confronted with data coming from other sources, particularly with the FBI's database on outstanding warrants for crime and violence. As regards this database the FBI has explicitly asserted that it has no obligation to ensure the accuracy of the data so processed. Therefore it might happen that travel would be denied to a person on the basis of false information.

The exaggerated duration of the data storage has created serious concerns regarding CAPPS II. However, it seems that the doubts have been, to a certain extent, dissipated (*supra*). Nevertheless, clarification has to be given regarding APIS.

The principle under analysis is in direct interdependence with the "purpose limitation" one, since whether the data processed is adequate, relevant and not excessive can only be determined in relation to the purpose.

Special attention has to be paid to sensitive data,[95] and the definition given to this concept. For instance, the definition given in the Safe Harbour Agreement differs from the one contained in the Directive. It is expected that in the future Agreement concerning passengers' data, respect be given to the definition of he Directive. The Undertakings express

The exaggerated duration of the data storage has created serious concerns

that "CBP and TSA are committed to filtering sensitive data (…)".[96] Specifications will have to be given concerning the characteristics of the filters to be implemented or design of SQL.

It is further stated that:

[w]ith respect to sensitive PNR data that has been transferred by air carriers to CBP, should it become necessary for CBP to use such sensitive data for purposes of preventing and combating terrorism and serious criminal offences, any such use will be subject to specific approval procedures, involving the US Deputy Commissioner of CBP, in consultation with the DHS Chief Privacy Officer.[97]

Can the EU accept this statement, considering that if these data has already been transferred, it was made in violation of the Directive?

The proportionality principle assessment, that is whether the data is adequate, relevant and not excessive, has to be complemented by a "necessity test", which normally evaluates to what extent the data kept is the only suitable and available means for the assurance of the purpose followed. The data is "necessary" if there is no other less invasive means to reach that purpose. The obligation under article 8 of the ECHR to adopt the less privacy intrusive measure has to be recalled in that context.

It is not possible to make a general statement about the implications of the "pull" and the "push" systems because the risks created for the protection of personal data depend on the modalities of implementation of those systems. For instance, it is obvious that, if what US authorities require is "full" access to PNR data, this system would be certainly far less respectful of data protection rights than the "transfer" of passengers' and crew manifests. Since the amount of data available would be limited in the second case, it would not include sensitive data, etc. However, if we think about the SQL, and the fact that code can be created to determine not only "who" is authorized to access, but also "what" he is entitled to do (only reading, reading and copy, etc) and regarding "which data" (the whole data base, only certain information, about certain persons, etc.), we can see that it can be an interesting way to limit access to sensitive data, or other data considered excessive. Furthermore, it would be possible to check whether unauthorized bodies or persons gain access by analysing the log files of the system.

In this regard, it would be also necessary to include a "sunset clause" to evaluate how the limits to the data protection rights created by those systems effectively contribute to the fight against terrorism.

(d) Restrictions on onward transfers:
The Decision to be adopted by the European Commission should be specific concerning the bodies (public or private) entitled to receive passengers' data and the responsibility they have. The Joint Statement is quite vague when saying:

(…) other law enforcement entities may specifically request PNR information from Customs and Customs, in its discretion, may provide such information for national security or in furtherance of other legitimate law enforcement purposes; for purposes of regulating the dissemination of PNR data which may be shared with other law enforcement entities, Customs is considered the 'owner' of the data and such entities are obligated by the terms of disclosure to obtain Customs express authorization for any further dissemination (sometimes referred to as the 'Third Agency Rule'); (…).

Again, the problem of purpose limitation is present here; "other legitimate law enforcement purposes" is really a very wide purpose that can include any kind of crime, which potentially violates the proportionality principle.

2. The right to a transparent and secure processing

(a) The "transparency" principle:
Passengers have to be provided with information about the purpose of the processing, their rights, as well as which US agencies are entitled to have access to their personal data. The application of this principle can be limited pursuant to Article 13 of the Directive. Any limitation to the right to be informed pursuant to Article 13.1 has to be clearly stated in order to evaluate the proportionality of the measure. Moreover:

[t]he Working Party underlines the necessity to have commitments from the US side that are officially published at least at the level of the Federal Register and fully binding on the US side.[98]

(b) The "security" principle:
The Annex to the Joint Statement specifies certain characteristics of the security measures. The measures mentioned are those adopted by Customs, but the document is silent concerning the measures adopted by the other bodies to which data are likely to be transferred/shared with.

(c) The "rights of access, rectification and opposition":

The Joint Statement affirms that:

[a]s concerns a first party request for disclosure of data by the data subject, US Customs will proceed with disclosure under the Freedom of Information Act (FOIA).

It would be advisable to create a standard form for access requests under the FOIA with translation to every Community language, considering that not every data subject who travels to the US, and whose data is required in a mandatory way, speaks English, or is able to understand how his rights can be enforced under the FOIA. Translation of the relevant information including the result of an access request would have to be assured, otherwise the data subject who does not speak English would not know whether he has to exercise his right to rectification or not.

Moreover, the Article 29 Data Protection Working Party[99] has expressed concern about the likelihood of the FOIA being used by third parties to access PNR data held by the US administration. This possibility has to be prevented.

(d) Independent authority and enforcement mechanisms:

There is a lack of clarity concerning what would be the legal remedies available to European data subjects to enforce their rights and, if necessary, obtain redress. Travellers need to know not only what the remedies are but also how affordable they are and what kind of assistance they are entitled to receive from public bodies. The system of State liability for misuse of data with EU origin has to be described in the document to be signed.

There is a strong need for an "independent body" to control the implementation of the data protection rules regarding EU passengers' data. Indeed, doubts remain concerning the independence of the DHS Chief Privacy Officer.

D. Conclusions

The Joint Statement and the Undertakings are obviously insufficient to regulate TBDF of passengers' data, both from a formal (they are not a source of Community law) and content (they are far from covering the requirements for an adequacy Decision) point of view.

With regard to the legal basis for EU actions, we reiterate what we have already expressed in the preliminary conclusions. A complementary approach between first and third pillars would have to be developed. Furthermore, whereas "access" should be ruled in the light of Article 4.1(c) of the Directive, "transfer" has to be ruled upon under Article 25 and 26. However, an adequacy Decision (Article 25.6) would be required to regulate transfers in both cases (in the case of an integral application of the Directive, as a result of the "transfer" made of "accessed" PNR data).

The way "access" is operated has to be thoroughly described, and limitations must be established concerning the categories of bodies/persons authorized, the categories of data that will be disclosed, and what will be the security measures to be implemented. Among others, controls in log files will permit follow-up of how "access" is exercised.

The purpose has to be delimited as precisely as possible, since many other parameters of the adequacy assessment have to be regarded *vis-à-vis* this principle (e.g. proportionality, transparency, security, etc.).

We strongly argue that the fight against terrorism and the protection of the right of individuals to be safe are *both* legitimate aspirations. The Directive and the *European Convention for the Protection of Human Rights and Fundamental Freedoms* offer legal instruments to balance the rights to privacy and personal data protection with them. Balancing conflicting rights in accordance with the rule of law (e.g. respecting legal parameters which proceed to limit any right) is one of the bases of the democratic system. The conflicting interests have to be interpreted, and the balance has to be made, in conjunction because otherwise contradictory and inapplicable results could arise.

María Verónica Pérez Asinari, Researcher and **Yves Poullet,** Dean of the Faculty of Law, Director of the CRID (*Centre de Recherches Informatique et Droit)* University of Namur

There is a strong need for an "independent body" to control the implementation of the data protection rules regarding EU passengers' data

Editor's Note:

The US General Accounting Office reported, in February 2004, that the CAPPS II initiative faces significant implementation challenges. See further: http://www.epic.org/privacy/airtravel/gao-capps-rpt.pdf An additional comment on this will appear in a future issue of CLSR.

Belgium, http://www.crid.be

This article expresses the own views of the authors. In no way might it be interpreted as the opinion of the organisations to which they belong.

We would like to thank Jean-Marc Dinant, researcher at the CRID, for his clarifying comments.

FOOTNOTES

1 In the EU, the fight against terrorism is one of the specific objectives mentioned in Article 29 TEU. The Framework Decision of 13 June 2002 on combating terrorism, OJCE L 164, 22.6.2002, has declared: "Whereas: (1) The European Union is founded on the universal values of human dignity, liberty, equality and solidarity, respect for human rights and fundamental freedoms. It is based on the principle of democracy and the principle of the rule of law, principles which are common to the Member States. (2) Terrorism constitutes one of the most serious violations of those principles. The La Gomera Declaration adopted at the informal Council meeting on 14 October 1995 affirmed that terrorism constitutes a threat to democracy, to the free exercise of human rights and to economic and social development. (…)".

2 107th Congress, 24 October 2001. The PATRIOT Act has been extensively analysed. Whereas certain sectors consider that it "eliminated the checks and balances that previously gave courts he opportunity to ensure that these powers were not abused" (Electronic Frontier Foundation "EFF Analysis of the Provisions of the USA PATRIOT Act", 31 October 2001, available at: http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.php , last visited 08/03/02), others argue that "the common wisdom on the USA Patriot Act is incorrect. The Patriot Act did not expand law enforcement powers dramatically, as its critics have alleged. In fact, the Patriot Act made mostly minor amendments to the electronic surveillance laws" (O. KERR "Internet Surveillance Law after the USA PATRIOT Act: the Big Brother that isn't", The George Washington University Law School, Public Law and Legal Theory Working Paper No. 043, available at: http://ssrn.com/abstract=317501).

3 Public Law 107-173, 107th Congress.

4 Ibid.

5 Department of Treasury, Customs Service, (66 FR 67482) T.D. 02-01.

6 Department of Treasury, Customs Service, (67 FR 42710) T.D. 02-33.

7 See on that concept the declaration made by A. Hutchinson, under-secretary of Border and Transportation Security at the US Department of Homeland Security, while referring to the US VISIT system as part of the comprehensive information system that will provide the United States with a "smart border" that "expedites legitimate trade and travel, but stops terrorists in their tracks". This system "will be based on visas that include biometric features such as fingerprints and photographs to permit identification of foreign visitors when they arrive. (…) Through this 'virtual border' we will know who violates our entry requirements, who overstays or violates the terms of their stay, and who should be welcome again". She further expressed that these initiatives must not be considered as a way to exclude any immigrants, "[i]mmigrants still search for the American Dream. And when they find it, all American benefit", reported in "Hutchinson says new system provides America with 'smart border'", web site of the US Mission to the E.U, 19 May 2003, available at : http://www.useu.be/Terrorism/USResponse/May1903USVISITSystem.html , last visited 08/08/03.

8 The TSA has been created under the ATSA.

9 Sec. 115. Passenger Manifest, paragraph (c). Amendment to 49 USC 44909.

10 The Interim rule of 31 December 2001 states that this transfer should be made "not later than 15 minutes after the departure of the aircraft from the last foreign port or place", p. 67483.

11 Sec. 115. Passenger Manifest, paragraph (c). Amendment to 49 USC 44909.

12See p. 67483.

13See p. 42710.

14 See p. 42711.

15 The history of PNR contains changes and deletions to a PNR from the date it was created (footnote added by the authors).

16 Under the PNR system, those fields are called SSR (Special Service Request).

17 For a practical description of PNR see: "Lesson: Passenger Name Record", Advanced Worldspan, available at: http://globallearningcenter.wspan.com/emealearningcenter/PDFs/Student%20Workbooks/210/1101%20PNR%20Lesson.pdf, last visited 02/09/03. See also: E. HASBROUCK "Total Travel Information Awareness", available at: http://hasbrouck.org/articles/travelprivacy.html, last visited 18/08/03. In this article we read: "Passenger Name Records (PNR's) maintained by airlines, computerized reservations systems or 'global distribution systems' (CRS's/GDS's), and travel agencies don't just contain flight reservations and ticket records. They include car, hotel, cruise, tour, sightseeing and theater ticket bookings among other types of entries. PNR's show where you went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a particular other person, they show whether you asked for one bed or two. Through departmental and project billing codes, business travel PNR's reveal confidential internal corporate and other organizational structures and lines of authority and show which people were involved in work together, even if they travelled separately. Particularly in the aggregate, they reveal trade secrets, insider financial information, and information protected by attorney-client, journalistic, and other privileges. Through meeting codes used for convention and other discounts, PNR's reveal affiliations – even with organizations whose membership lists are closely-held secrets not required to be divulged to the government(…)". More specifically on PNR, by the same author, see: "What's in a Passenger Name Record (PNR)?", available at: http://hasbrouck.org/articles/PNR.html, last visited 18/08/03.

18 Planned to be implemented from January 2004.

19 $400 million have been foreseen by the Congress to set up the system.

20 For a European view regarding biometrics see: Article 29 Data Protection Working Party, Working Document on biometrics, 1st August 2003, WP 80, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf

21 On all that see "Hutchinson says…", op.cit.

22 In fact, documents obtained by EPIC demonstrate the existence of two lists: the "No-Fly" watchlist and the "selectee" list regarding persons submitted to additional security measures. The criteria for putting a name into

the list remain secret. See: EPIC "Documents show errors in TSA's 'No-Fly' watchlist", April 2003, available at: http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html , last visited 08/08/03.

23 The first CAPPS has been created after the Lockerbie bombing of a PanAM jet.

24 Statement of Admiral James M. Loy, Administrator of the Department of Homeland Security's Transportation Security Administration, before the House of Representatives Subcommittee on Technology and Information Policy, 6 May 2003, available at : http://www.useu.be/Terrorism/USResponse/May0603LoyITTransportSecurity.html, last visited 08/08/03.

25 Ibid., available at: http://www.useu.be/Terrorism/USResponse/May0603LoyITTransportSecurity.html, last visited 08/08/03. It has to be noted that from a European perspective, as we will see later on, the implementation of security measures is one of the obligations of data controllers, but certainly not the only one.

26 This person is N.O'Connor Kelly, who was present at the Hearing organized by the European Parliament. She insisted on the fact that the creation of this position was a "historic development in privacy and data protection in US" insofar it marks the "first statutorily mandated, Congressopnally created privacy officer for the Department of Homeland Security (…)", see the report at the United States Mission to the European Union website "US Officials Discuss Homeland Security, passenger name Record with EU", available at: http://www.useu.be/Terrorism/USResponse/May0603BrowingPNREP.html , last visited 08/08/03.

27 The airline companies are subject to penalties in case they do not comply with the different US provisions.

28 See the report "Hutchinson says new system provides America with 'smart border'", op. cit.

29 About ECHELON see the Federation of American Scientists' website: http://www.fas.org/irp/program/process/echelon.htm. And the report Y. POULLET and J.M. DINANT, "Le réseau Echelon existe t'il ? Que peut-il faire ? Peut-on et doit-on s'en protéger ?" Report published by the Belgian Committee of Surveillance, 1999, p. 13 and ss., available at: http://www.droit.fundp.ac.be/textes/echelonfr.pdf.

30 See the European Parliament Resolution , 5 September 2001 and the Working Paper of the European Parliament temporary Committee on the Echelon Interception System (Schmidt Report), available at: http://fas.org/irp/program/process/europarl.draft.pdf.

31 Department of Homeland Security, Transportation Security Administration, Docket No.DHS/TSA-2003-1, Privacy Act of 1974: Notice of Status of System of Records; Interim Final Notice; Request for Further Comments, (68 FR 45265).

32 Testimony of Barry Steinhardt, Director of the ACLU Technology and Liberty Program on Government Data Mining Before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, available at: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12669&c=206 , last visited 04/09/03.

33 See the EPIC's website : http://www.epic.org/privacy/intl/passenger_data.html , last visit 22/08/03.

34 EPIC v. DHS, TSA and DoD; United States District Court for the District of Columbia, available at: http://www.epic.org/privacy/airtravel/capps2-suit.pdf , last visited 02/09/03.

35 John Gilmore v John Ashcroft et al, United States District Court Northern District of California, available at: http://cryptome.org/gilmore-v-usa-cid.htm, last visited 18/08/03.

36 (1) Vagueness in Violation of the Due Process Clause of the Fifth Amendment of the United States; (2) Violation of the Right to be Free from Unreasonable Searches and Seizures in Violation of the Fourth Amendment of the United States Constitution; (3) Violation of the Right to Travel in Violation of the Due Process Clause of the Fifth Amendment of the United States Constitution; (4) Violation of the Right to Travel and Associate Anonymously in Violation of the First and Fifth Amendment of the United States Constitution; (5) Violation of the Right to Petition the Government for Redress of Grievances in Violation of the First Amendment of the United States Constitution; (6) Violation of the Right to Equal Protection in Violation of the Fifth Amendment of the United States Constitution.

37 E. HASBROUCK "Establishment and Exemption from the Privacy Act of Records System DOT/TSA 010, 'Aviation Security-Screening Records (ASSR)'", 23 February 2003, available at: http://hasbrouck.org/articles/Hasbrouck_DOT_comments-23FEB2003.pdf , last visited 02/09/03.

38 Pending Bills dealing with CAPPS II have been object of different Amendments issued by members of the US Senate and the US House of Representatives. See: the Wyden Amendment, available at: http://www.epic.org/privacy/airtravel/wyden_capps_amdt.pdf , last visited 02/09/03; the Sabo Amendment, available at: http://www.house.gov/sabo/pr03-18.htm , last visited 02/09/03.

39 As well as from European civil liberties advocates. See, for instance, the "Campaign against the illegal transfer of European travellers' data to the USA" organised by EDRI (European Digital Rights), information available at: http://www.edri.org/cgi-bin/index?funktion=view&id=000100000085 , last visited 08/08/03.

40 Convention for the Protection of Human Rights and Fundamental Freedoms ETS no.: 005, Rome 4/11/50. Available at: http://conventions.coe.int/treaty/en/WhatYouWant.asp?NT=005

D. YERNAULT "L'efficacité de la Convention Européenne des Droits de l'homme pour contester le système 'Echelon' ", in Sénat et Chambre des Représentants de Belgique, Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé 'Echelon' , 25 Feb. 2002. In this article, the author studies the nature of the ECHR: (1) as an instrument guaranteeing "European public order", considered as a coherent whole, in the sense that it was qualified by the Strasbourg Court in 1995; (2) as an international treaty that gives place to the State's international liability; and (3) as an international treaty of a particular nature, due to its Article 53, by virtue of which adherent States recognise its legal pre-eminence over any other internal or international regulation that would be less protective of Fundamental Rights than the Convention itself.

41 Case Amann v. Switzerland (Application n. 27798/95), Strasbourg, 16 February 2000; Case Rotaru v. Romania (Application n. 28341/95), Strasbourg, 4 May 2000; Case P.G. and J.H. v. The United Kingdom (Application n. 44787/98), Strasbourg, 25 September 2001, etc.

42 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no.:108, Strasbourg 28-01-1981. Available at: http://conventions.coe.int/treaty/en/Treaties/Html/108.htm

43 Among others: Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999); Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997); Recommendation

No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991); Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations (13 September 1990); Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987), etc.

44 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEC L 281 , 23/11/1995, p. 31 – 50, hereinafter: "the Directive".

45 Full text of the Charter of fundamental Rights of the European Union, OJEC C 364/1, 18-12-200: http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf. See also: Article 29 Data Protection Working Party, Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights, 7th September 1999, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp26en.htm

46 See on that point, our reflections published in Y. POULLET, "Pour une justification …", op.cit., p. 240.

47 See: L. BYGRAVE "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", International Journal of Law and Information Technology, vol. 6 no. 3. This paper examines the extent to which the basic principles of data protection laws may be read into provisions in human rights treaties proclaiming a right to privacy.

48 For a more in-depth analysis of the articles 7 and 8 of the Charter and the significance of the distinction between data protection and privacy, Y. POULLET, "Pour une justification …", op.cit., p. 277 and 278.

49 Submitted to the President of the European Council in Rome on 18th July 2003, available at: http://european-convention.eu.int/docs/Treaty/cv00850.en03.pdf , last visited 29/08/03.

50 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector; OJEC L 024 , 30/01/1998, p. 1 – 8.

51 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJEC No L 201, 31 July 2002. Article 3 §1 states: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". PNR system would not fall under this category. On the scope of application of the new Directive see: S. LOUVEAUX and MV. PEREZ ASINARI "New European Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector. Some initial remarks", Computers and Telecommunications Law Review, volume 9, issue 5, 2003, p. 133-138.

52 Article 3 of the Directive.

53 Article 2(d) of the Directive.

54 Article 4.1(a) of the Directive.

55 We will analyse the "purpose" infra.

56 In this regard see the Article 13 of the Agreement on extradition between the European Union and the United States of America, OJEC L 181/27, 19.07.2003.

57 We read in the point (43) of the Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration: "[i]n the event that the European Union decides to adopt an airline passenger identification system similar to that of the US Government, which requires all air carriers and GDSs to provide European authorities with access to PNR data for persons whose current travel itinerary includes a flight to, from, through or within the European Union, CBP and TSA would encourage US based airlines to cooperate".

58 The Europol Convention has its own regulation on personal data protection, as well as specific rules dealing with TBDF, requiring also "adequacy" in the third country in question.. See article 18 of the Europol Convention adopted by Act of Council on 26 July 1995, OJEC C 316, 27.11.1995. However for the transfer of passengers' data, as we have already said, EU public bodies do not intervene. Yet, this Convention was adopted in the context of ex-Article K.3 (current 31 TEU), what reveals that the concept of "adequacy" is neither unknown nor irrelevant in the third pillar sphere.

59 We have to bear in mind that otherwise, member States would be subject to liability for violation of the ECHR. See on that point, D. YERNAULT "L'efficacité de la Convention Européenne des Droits de l'homme…", op. cit.

60 In fact, this aspect goes beyond TBDF, and consists in an exploration concerning how far the requirements themselves will influence the legal basis: first pillar (Articles 25/26 or 4.1 (c) of the Directive), second pillar, third pillar of EU law. See infra for this analysis.

61 Article 25.2 of the Directive.

62 Article 26.1 of the Directive.

63 The impossibility to use those derogations in the context of the transfer of travellers' personal data by air companies to the US as a general rule has been clearly explained by the Article 29 Data Protection Working Party. See its Opinion 6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States, 24 October 2002, WP 66, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2002.htm

64 See also Recitals 43, 44, and 45 of the Directive.

65 "The interference was not therefore 'in accordance with the law' as required by the second paragraph of Article 8 and there has been a violation of this provision. In these circumstances, an examination of the necessity of the interference is no longer required", European Court of Human Rights, case P.G. and J.H. v. The United Kingdom (Application n. 44787/98), Strasbourg, 25 September 2001, p. 17. "The Court concludes that the interference cannot therefore be considered to have been 'in accordance with the law' since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration. (...) Having regard to the foregoing conclusion, the Court does not consider it necessary to examine whether the other requirements of paragraph 2 of Article 8 were complied with", European Court of Human Rights, case Amann v Switzerland (Application n. 27798/95), Strasbourg, 16 February 2000, p. 19. See also: Vincent COUSSIRAT-COUSTERE "Article 8 § 2", in La Convention Européenne des Droits de l'Homme. Commentaire article par article, Louis PETTITI, Emmanuel DECAUX et Pierre IMBERT (eds), Economica, 2e Edition, Paris, 1999, p. 323-351.

66 The same debate has been held as regards the exchange of personal data between Europol and the US just after the 11 September tragic events. After long debate the JHA Council has approved a draft agreement between US and EU on 19 December 2002. On this agreement and certain concerns expressed on its legitimacy, see the report of the EU Network of

Independent Experts in Fundamental Rights, "The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats", Thematic Comment drafted upon request of the European Commission, DG Justice and Home Affairs, Unit A5, submitted on 31 March 2003, p. 24, available at: http://www.statewatch.org/news/2003/apr/CFR-CDF.ThemComment1.pdf , last visited 08/08/03.

67 Article 26.2 of the Directive.

68 Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC - OJEC L 181/19 of 4.7.2001, available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf

69 Commission Decision 2002/16/EC of 27 December 2001on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC- OJEC L 006 of 10.01.2002, p. 52 – 62, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-16_en.pdf

70 Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce - OJEC L 215/7 of 25.8.2000.

71 It has to be noted that not only European airline companies are subject to the Directive 95/46/EC, but every company processing personal data in the EU.

72 The Article 29 Data Protection Working Party has expressed the same view in this particular issue. See Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States, 24 October 2002, WP 66, p. 7. Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 13 June 2003, WP 78, p. 7. For a clarification on "applicable law" issues see: Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 30 May 2002, WP 56. See also, on the application of Article 4.1(c): MH. BOULANGER and C. de TERWANGNE "Internet et le respect de la vie privée", in Cahiers du Centre de Recherches Informatique et Droit, n . 12, 1997, p. 211.

73 Article 2(d) of the Directive.

74 The Annex to the Joint Statement adds that "The United States Customs Service represents that: by legal state (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), air carriers operating passenger flights in foreign air transportation to, from or through the United States, must provide with electronic access to PNR data contained in the automated reservation/ departure control systems ('reservation systems')". In the following paragraphs the idea of "access" is reinforced: "with regard to the PNR data which Customs accesses directly from the air carrier's reservation systems, Customs will only view PNR data concerning persons whose travel includes a flight into, out of or through the United States; Customs will access air reservation systems as an accommodation to the air carriers to obviate the need for costly technical changes required to allow the air carriers to transmit the data to Customs". Italics have been added by the authors.

75 This is a role that would certainly not be assumed by the US Embassy for reasons of Public International law.

76 Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States, 24 October 2002, WP 66, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2002.htm

77 Article 29 Data Protection Working Party, Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, 14 December 2001, WP 53, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp53en.pdf

See also: EU Network of Independent Experts in Fundamental Rights, "The Balance between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats", Thematic Comment drafted upon request of the European Commission, DG Justice and Home Affairs, Unit A5, submitted on 31 March 2003.

78 The Joint Statement has been published on the website of the European Commission (DG External Relations): European Commission: US Customs talks on PNR transmission, Joint Statement, Brussels, 17/18 February 2003, available at: http://europa.eu.int/comm/external_relations/us/intro/pnr.htm

79 At the longer run, both parties agreed on the necessity of a multilateral agreement under the umbrella of International Civil Aviation Organization (ICAO).

80 The letter recalls that national Data Protection Authorities are not free to apply or not the data protection legislation and "it has not yet been clarified how the Joint Statement might provide a sound legal basis to justify an exception to the rule."

81 Different hearings have been held by the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. The first one took place on 25 March 2003; another one on 6 May 2003.

82 European Parliament, Motion for a Resolution on transfer of personal data by airlines to the US immigration service, 6th March 2003, B5-0000/2003.

83 European Parliament, Motion for a Resolution…, p. 3.

84 Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 13 June 2003, WP 78, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2003.htm

85 The sources of Community law are strictly described in Article 249 of the TEC.

86 Article 29 Data Protection Working Party, Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 24th July 1998, WP 12, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm

87 Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration, available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78-pnrf-annex_en.pdf

88 See the proceedings of the Conference "Les attentats du 11 septembre 2001: Conséquences géopolitiques mondiales et lutte anti-terroriste", Département culturel des Facultés Universitaires Notre-Dame de la Paix de Namur, November 2001.

89 This principle has been constantly repeated by the European Court of Human Rights in what concerns electronic surveillance and wire tapping [see notably recently, Klass and others v Germany (Series A n. 28), Strasbourg 6 September 1978, Khan v U.K (Application n. 35394/97) Strasbourg 12 May 2000]

90 The European Court of Human Rights has developed its case-law particularly as regards the monitoring of communications, but it seems to us that the same reasoning might be done as regards other data.

91It should be clear, before any decision be adopted by EU authorities, which is the definition of "terrorism" and any other relevant concept mentioned as the purposes of US authorities for the processing of personal data with EU origin. This issue seems to be problematic even in the EU side: "[n]either international legal instruments, nor the Framework Decision of the Council on 13 June of 2002 concerning the fight against terrorism have really succeed in overcoming the difficulties traditionally encountered when attempting to give a definition of terrorism which describes its specificity, compared to other forms of organized crime in relation to all its possible forms. However, a sufficiently exact definition of the offence of terrorism is a prerequisite not only for specific indictment, but also for the application of specific procedural rules, particularly in the context of the inquiry of the investigation, and even more so for special forms of detention; otherwise the measures adopt in the fighting terrorism will lack clear legal basis, potentially bringing into question their lawfulness". EU Network of Independent Experts in Fundamental Rights, "The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats", Thematic Comment drafted upon request of the European Commission, DG Justice and Home Affaires, Unit A5, submitted on 31 March 2003, p. 7. See the analyses on this specific problem made in pages 11-16. See the definitions given in Articles 1 and 2 by the Framework Decision of 13 June 2002 on combating terrorism, OJCE L 164, 22.6.2002, p.4. See also the Opinion of the Economic and Social Committee on the 'Commission Working Document – The relationship between safeguarding internal security and complying with international protection obligations and instruments', 2002/C 149/09, OJCE C 149, 21.6.2002, specially points 2.7, 2.9, 2.1. A draft global Convention against terrorism is currently being negotiated within the United Nations.

92 Certain concerns might be expressed about the possible use of PNR records for ensuring a better control on immigration (see the possible links with the USVISIT program).

93 On the EU side, lists including persons and entities linked to terrorism are being made. See: Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with the view to combating terrorism, OJEC L 344, 28.12.2001. Article 2.3 states that "The Council, acting by unanimity, shall establish, review and amend the list of persons, groups and entities to which this Regulation applies, (…)".

94 E.HASBROUCK, "What's wrong with CAPPS-II ?", available at : http://hasbrouck.org/articles /CAPPS-II.html , last visited 18/08/03.

95 Even if the WP n. 12 does not include it in this principle we can certainly connect it with the "proportionality principle".

96 Undertakings, point (8).

97 Undertakings, point (9).

98 Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 13 June 2003, WP 78, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2003.htm

99 Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 13 June 2003, WP 78, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs-2003.htm